CSA STAR

Your implementation guide

bsi.

...making excellence a habit.™

What is **CSA STAR**?

With predictions that more than $1 trillion in IT spending will be directly or indirectly affected by the shift to cloud by 2020[1], organizations need to ensure they maximize their investments and have confidence in their cloud service provider. That's where best practice frameworks like CSA STAR can help.

Based on a control set that was created and is owned by the Cloud Security Alliance (CSA), our **CSA STAR** certification supports cloud service providers (CSPs) to enhance their ability to maintain data confidentiality, integrity and availability in the cloud.

As co-authors of **CSA STAR**, we have the experience, the experts and the support services to help make sure you get the most from **CSA STAR,** making you more agile and secure in the changing digital environment.

This guide shows how you can apply the control set in your organization to remain resilient over the long term, reassuring clients and supporting business growth. We also showcase our additional support services, which help you not only achieve certification, but continue to deliver a quality service, reduce risk and protect your business

"By achieving compliance to CSA STAR, the most comprehensive cloud security standard to date, users can rest assured relying on Ribose for their success."

Ronald Tse, Ribose, Hong-Kong based cloud service provider

Contents

What does **CSA STAR** deliver for you and your company

CSA STAR addresses issues specific to cloud computing through the control set known as the cloud control matrix (CCM). It provides organizations with a useful tool for reviewing their compliance against a wide range of cloud-based standards and industry best practices. This helps increase security, trust and assurance in the services offered, giving users a key differentiator when selecting their Cloud Service Provider (CSP).

Benefits of CSA STAR

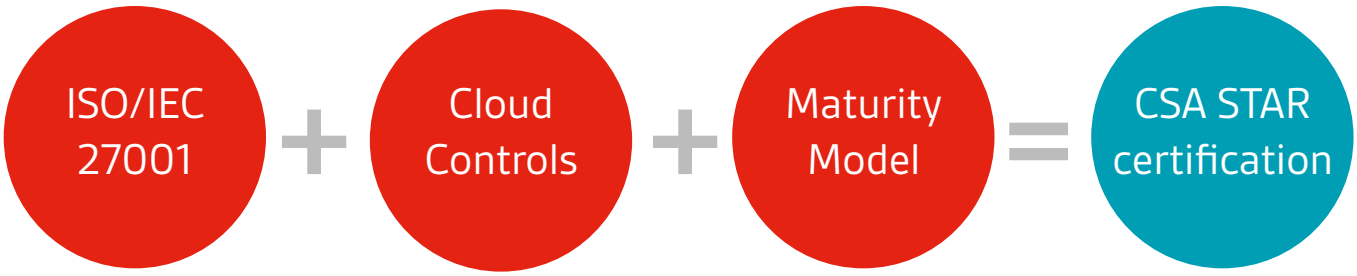
- Provides a competitive advantage
- Shows commitment to best practice and drives maturity optimization
- Inspires trust and customer assurance
- Enhances cloud security controls

"CSA STAR is a very big differentiator. We can stand toe-to-toe with our biggest competitors."

Dan Timko, Cirrity, US-based cloud service provider

How does **CSA STAR** work?

CSA STAR certification builds upon an ISO/IEC 27001 information security management system. It involves being assessed against additional controls outlined in the CSA Cloud Controls Matrix (CCM). It also contains a management capability (maturity model) which gives CSPs a benchmark model for managing and analysing the performance of their cloud services to support with continually driving improvement.



What is ISO/IEC 27001?

ISO/IEC 27001 sets out the requirements for the information security management system (ISMS). Internationally recognized, it's an excellent framework which helps organizations manage and protect their information assets so they remain safe and secure.

By embedding an **ISO/IEC 27001** system you can better identify risks and put in place the security measures that are right for your business. Building in the additional controls with CSA STAR, you can ensure you have also addressed risks specific in the cloud environment. This will give you confidence that you are protecting your business, your reputation and adding value.

Cloud Control Matrix

The CSA regularly review the CCM to ensure it remains up-to-date with industry best practice. It's widely adopted by leading cloud service providers and other organizations that have a dedicated focus on cloud services and the resources to regularly adapt.

Key requirements of CSA STAR

The CSA STAR framework provides 16 control areas that align with 5 capability factors.

Capability factors

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

Control areas

AIS	Application and Interface Security
AAC	Audit Assurance and Compliance
BCR	Business Continuity Management and Operational Resilience
CCC	Change Control and Configuration Management
DSI	Data Security and Information Lifecycle Management
DSC	Datacentre Security
EKM	Encryption and Key Management
GRM	Governance and Risk Management
AIS	Human Resources Security
IAM	Identity and Access Management
IVS	Infrastructure and Virtualization
IPY	Interoperability and Portability
MOS	Mobile Security
SEF	Security Incident Management, E-Disc and Cloud Forensics
STA	Supply Chain Management, Transparency and Accountability
TVM	Threat and Vulnerability Management

A performance score is given to each capability factor for every control area to indicate the maturity of the system and how well it is managed. There are clear criteria for each individual score that allow a maturity rating to be provided. 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 is effective.	Stakeholders are systematically identified, and consulted with effective communication.	Stakeholders are actively engaged in improving measures and understand how changes effect them	Relevant stakeholders monitor and measure processes and how they need to develop to meet the strategic objectives

Our assessment process will provide you with a score, which will help you to identify areas for improvement and enhance your offering to clients.

You can download the cloud control matrix from the CSA website, along with a useful self-assessment tool to help you work through the controls and identify any gaps before your assessment.

Top tips on making **CSA STAR** effective for you

Every year we help tens of thousands of clients. Here are their top tips.

Top management commitment is key to making implementation of CSA STAR a success

"With some organizations remaining wary of cloud services due to security and privacy concerns, Exponential-e's achievement of CSA STAR is a pioneering step forward for the whole cloud industry."

Jitesh Bavisi, Exponential-e, UK-based cloud service provider

Think about how **different departments work together** to avoid silos. Make sure the organization works as a team for the benefit of customers and the organization.

"It is very clear that we will benefit from harmonizing our security efforts into a single program. We don't want to spend a lot of time preparing for, or going through, audits. Doing everything together makes our lives much easier."

Dan Timko, Cirrity, US-based cloud service provider

Review systems, policies, procedures and processes you have in place – you may already do much of what's in the standard, and make it work for your business.

"With CSA STAR Certification, customers can gain confidence that Microsoft Azure is meeting customer needs and relevant regulatory requirements, as well as actively monitoring, measuring and continually improving the effectiveness of our management system."

Alice Rison, Microsoft Azure, global public cloud platform

Speak to your customers and suppliers. They may be able to suggest improvements and give feedback on your service.

"Our customers want to know that we are 'doing security right', and in a market where the number of vendors is increasing, they need confidence they are selecting the best vendor for their needs."

Fergus Kennedy, Pulsant, UK-based cloud hosting provider

Train your staff to carry out internal audits of the system. This can help with their understanding, but it could also provide valuable feedback on potential problems or opportunities for achievement.

Implementing the requirements is about improving the business, not just fighting for the badge. We have definitely learned from the process."

Fergus Kennedy, Pulsant, UK-based cloud hosting provider

And finally, when you gain certification celebrate your achievement and use the **BSI Assurance Mark** on your literature, website and promotional material.

bsi. CSA STAR Cloud Security

Your **CSA STAR** Journey

Whether you're new to CSA STAR or looking to enhance your current system, we have the right resources and training courses to help make sure it delivers the best for your business.

	You need to:	We help you:
Understand and prepare	• Download the cloud control matrix (CCM) and read it; understand the content, your requirements and how it will improve your business • Contact us, we can propose a solution that aligns to your organization's needs	• Download the cloud control matrix from the CSA website • Discover information on our website, including case studies, whitepapers and webinars visit **bsigroup.com/en-nz** • Attend a BSI In-house Introduction to CSA STAR training
See how ready you are	• Ensure your organization understands the principles of CSA STAR and the roles individuals will need to play, and review your activities and processes against the CCM	• Attend BSI Auditing cloud security for CSA STAR certification training • Book a BSI gap assessment to see where you are • BSI Entropy™ Software can support your CSA STAR implementation
Review and get certified	• Contact us to book your certification assessment	• Attend BSI Advanced cloud security auditing for CSA STAR certification training • BSI Entropy™ Software helps you effectively manage your system • Your BSI certification assessment

Continually improve and make excellence a habit

Your journey doesn't stop with certification. We can help you to fine-tune your organization so it performs at its best.

- Celebrate and promote your success – download and use the BSI Assurance Mark to show you are certified.
- Use BSI Entropy™ Software to help you manage systems and drive performance.
- Your BSI Client Manager will visit you regularly to make sure you remain compliant and support your continual improvement.
- Consider integrating other management systems standards to maximize business benefits such as ISO 9001 Quality Management and ISO 14001 Environmental Management.

BSI Training Academy

Boost your knowledge with our expertise: BSI has a comprehensive range of training courses to support you to work with CSA STAR. Our expert tutors can transfer the knowledge, skills and tools your people need to embed the framework of excellence into your organization. What's more, the accelerated learning techniques applied in our courses will help make sure that what you learn stays with you.

Courses that help you understand CSA STAR include:

Introduction to Cloud Security and CSA STAR Certification

- One-day classroom based training course
- Learn about the structure and key requirements of CSA STAR and the cloud control matrix
- Essential for anyone involved in the planning or managing cloud services

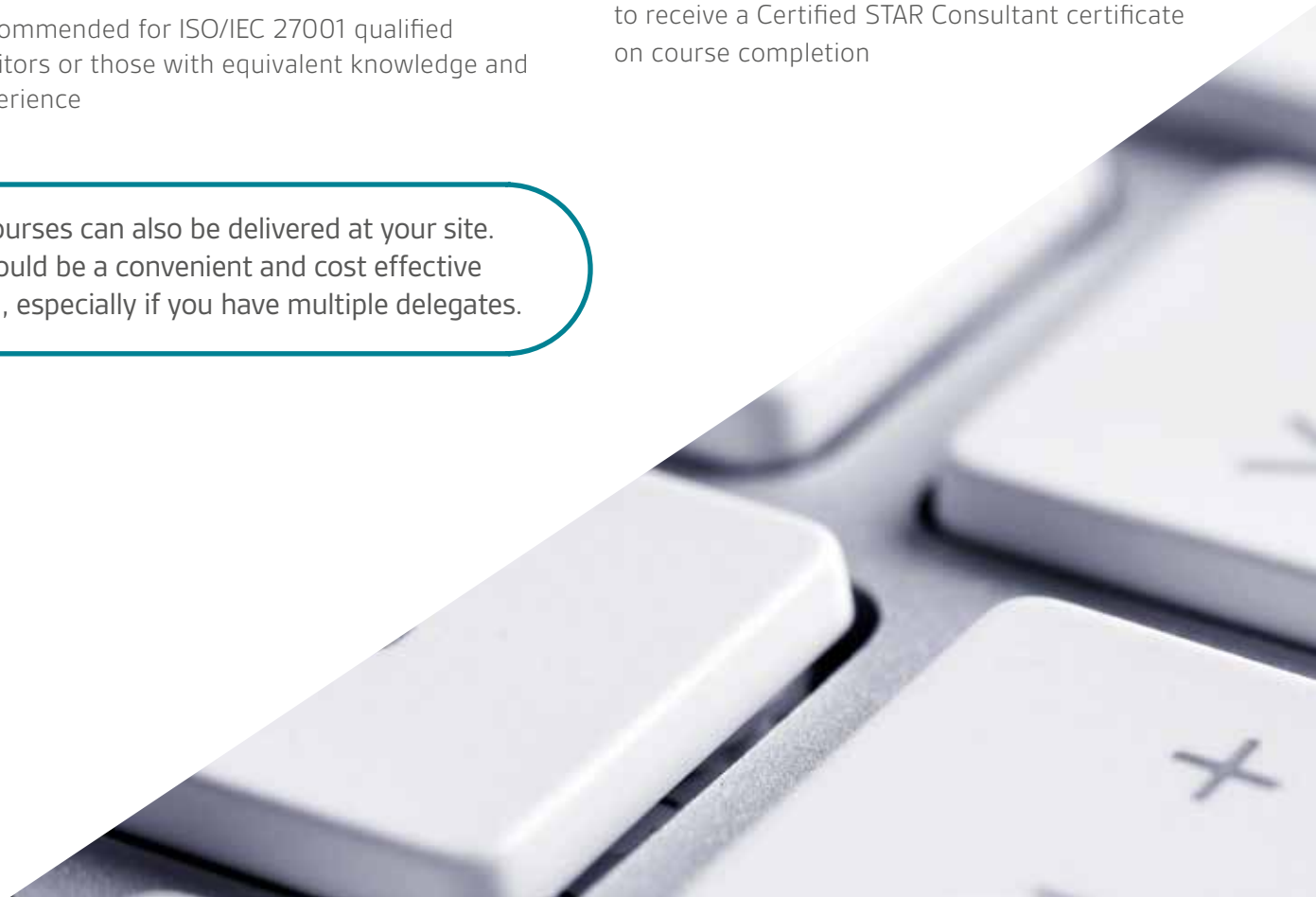
Auditing Cloud Security for CSA STAR Certification

- One-day classroom based training course
- Discover how to apply the cloud control matrix and effectively prepare a cloud service provider for a CSA STAR audit
- Recommended for ISO/IEC 27001 qualified auditors or those with equivalent knowledge and experience

Advanced Auditing Cloud Security for CSA STAR Certification

- Two-day classroom based training course. Combines the one-day Auditing Cloud Security for CSA STAR Certification training with an extra day focusing on the maturity score rating
- Learn how to effectively prepare an organization for a CSA STAR audit and understand how the CSA STAR maturity is determined
- Ideal for anyone involved in conducting an internal or second-party audit of CSA STAR frameworks or consultants working with organizations to embed CSA STAR
- Consultants attending this course are also eligible to receive a Certified STAR Consultant certificate on course completion

Our courses can also be delivered at your site. This could be a convenient and cost effective option, especially if you have multiple delegates.



BSI Entropy™ Software

Accelerate implementation time and deliver continual improvements

The decision to enhance a management system standard is a huge opportunity to drive business improvement, but initiating, implementing and maintaining this can also be a challenge. Ensuring you get the most from your investment is a key driver to your future success.

BSI Entropy™ Software provides a solution that can significantly reduce the cost and effort to implement frameworks, such as CSA STAR. It can be configured to the requirements of CSA STAR and provide your organization with the tools necessary to manage it across your organization. The start of your CSA STAR journey is an ideal time to implement BSI Entropy™ Software to support your management of cloud security.

It can help you to:

- Accelerate implementation time by up to 50%
- Manage your document control effectively
- Provide company-wide visibility on implementation of the standard so you know exactly where you are at any one time
- You can easily and accurately input actions related to audits, incidents/events, risk and performance
- Through its customizable dashboards and reporting tools it gives you early insight into trends that help you make business decisions early on and drive improvement

The savings are the costs you avoid because you could not see what was happening at the facility level.

Why BSI?

By Royal Charter

CSA STAR Cloud Security

BSI has been at the forefront of information security standards since 1995, having produced the world's first standard, BS 7799, now ISO/IEC 27001, the world's most popular information security standard. And we haven't stopped there, addressing the new emerging issues such as cyber and cloud security. That's why we're best placed to help you.

At BSI we create excellence by driving the success of our clients through standards. We help organizations to embed resilience, helping them to grow sustainably, adapt to change, and prosper for the long term. We make excellence a habit.

For over a century our experts have been challenging mediocrity and complacency to help embed excellence into the way people and products work. With 80,000 clients in 182 countries, BSI is an organization whose standards inspire excellence across the globe.

Our products and services

We provide a unique combination of complementary products and services, managed through our three business streams; Knowledge, Assurance and Compliance.

Knowledge

The core of our business centres on the knowledge that we create and impart to our clients. In the standards arena we continue to build our reputation as an expert body, bringing together experts from industry to shape standards at local, regional and international levels. In fact, BSI originally created eight of the world's top ten management system standards.

Assurance

Independent assessment of the conformity of a process or product to a particular standard ensures that our clients perform to a high level of excellence. We train our clients in world-class implementation and auditing techniques to ensure they maximize the benefits of standards.

Compliance

To experience real, long-term benefits, our clients need to ensure ongoing compliance to a regulation, market need or standard so that it becomes an embedded habit. We provide a range of services and differentiated management tools to facilitate this process.

bsi.

Find out more
Call: 0800 583 965
Visit: bsigroup.com/en-nz

© BSI group BSI/NZ/1071/SC/0417/EN/BLD