...making excellence a habit.™

Build confidence in the cloud

Best practice frameworks for cloud security

Cloud services are rapidly growing and becoming more of a focus for business.

It's predicted that more than $1 trillion in IT spending will be directly or indirectly affected by the shift to the cloud during the next five years[1]. This is no surprise as the cloud is one of the main digital technologies developing in today's fast-moving world. It's encouraging that CEOs recognize that it's crucial for them to champion the use of digital technologies[2] to keep up with today's evolving business environment. There are, however, still concerns over using cloud services and the best approach for adoption. That's where BSI can help.

We recognize that responding to emerging technologies can be difficult, especially with an ever-growing variety of products and services. As a business improvement partner, we work with clients to understand key drivers and help select the best practice approaches that suit their organization and build greater resilience.

This guide is designed to help you understand the different best practice frameworks to build a secure cloud environment.

What influences cloud adoption?

Choosing an approach

Business strategy and objectives should help organizations decide the best approach to cloud computing. This may involve using public cloud services, a private cloud or a hybrid cloud solution. It will often be influenced by your resources and priorities.

Public cloud	Private cloud	Hybrid cloud
An internet based service where information from a number of different organizations may be stored together	A service based on an organization's private network	Where a combination of different cloud services is used by an organization

Tackling the barriers

- Security concerns still top the list as a barrier to cloud adoption[1], particularly with public cloud provisions
- 73% of IT professionals say the biggest obstacle to cloud projects is the security of data[3]
- 91% of organizations are very or moderately concerned about public cloud security[4]

This isn't just within IT departments, 61% of IT professionals believe the security of data residing in the cloud is an executive concern[3]. This is critical considering the variety of cloud services that support the wider business operations, such as CRM systems, HR self-service portals and business complaint systems, to name a few.

Getting executive buy-in can help align cloud service offerings and improve delivery. Plus, it can support instilling a best practice approach to security throughout the business, ensuring all employees are trained on how to recognize information security threats and the action they need to take to support the business.

The benefits

Cloud services can provide a number of benefits including:

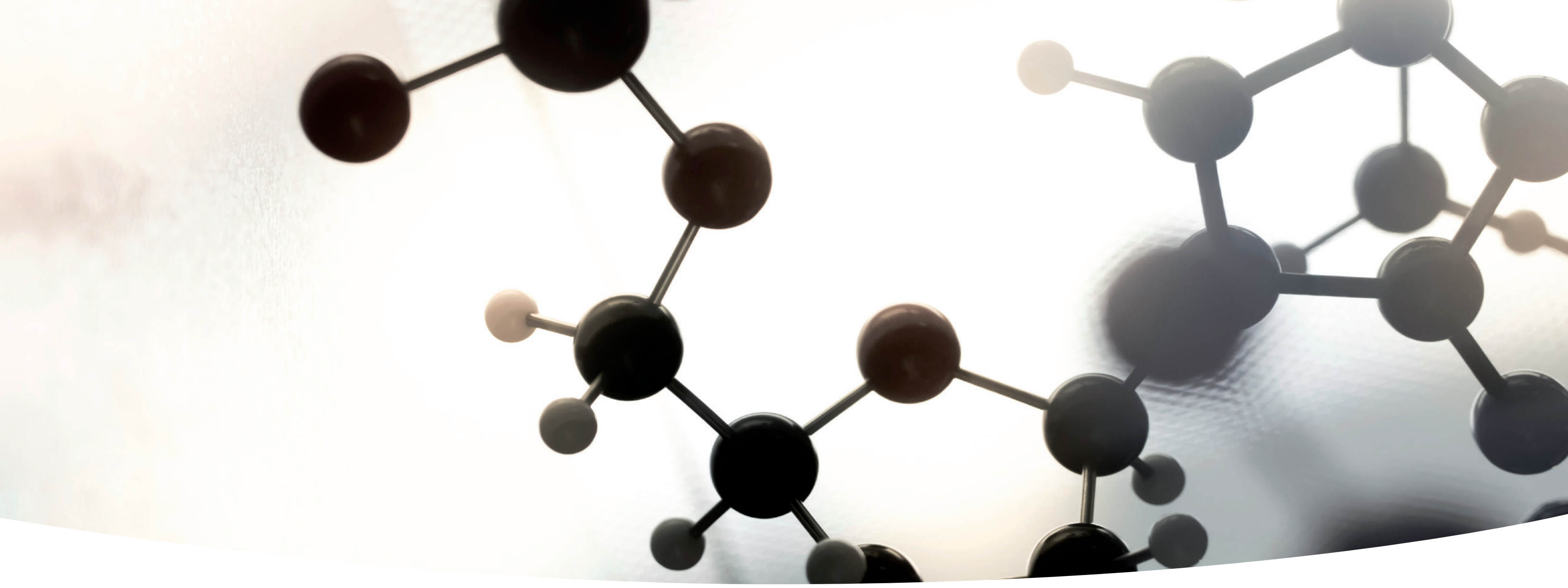
- **Agility**: you can respond more quickly and adapt to business changes
- **Scalable**: cloud platforms are less restrictive on storage, size, number of users
- **Cost savings**: no physical infrastructure costs or charges for extra storage, exceeding quotas, etc.
- **Enhanced security**: standards and certification can show robust security controls are in place
- **Adaptability**: you can easily adjust cloud services to make sure they best suit your business needs
- **Continuity**: organizations are using cloud services as a back-up internal solution

[1] Gartner, Market Insight: Cloud Shift — The Transition of IT Spending from Traditional Systems to Cloud, July 2016

[2] PWC Digital IQ report 2015

[3] Cloud Security Alliance: Cloud Adoption Practices and Priorities Survey Report 2015

[4] Information Security Community – LinkedIn, Cloud-Security-Report-2016



Solutions to help you manage cloud security

We have a range of products and services that focus on putting appropriate frameworks and controls in place to manage cloud security.

ISO/IEC 27001

The international standard for an Information Security Management System (ISMS).

ISO/IEC 27001 is the foundation of all our cloud security solutions. It describes the requirements for a best practice system to manage information security including understanding the context of an organization, the responsibilities of top management, resource requirements, how to approach risk, and how to monitor and improve the system.

It also provides a generic set of controls required to manage information and ensures you assess your information risks and control them appropriately.

It's relevant to all types oforganizations regardless of whether they are involved with cloud services or not, to help with managing information security against recognized best practice.

BSI provides top quality training to ensure you maximize the benefits of ISO/IEC 27001 and we also provide certification services.

ISO/IEC 27002

A code of practice for security controls. It provides more detail on the generic security controls, which organizations might wish to apply when implementing a management system, such as ISO/IEC 27001, ISO/IEC 27017 and ISO/IEC 27018.

ISO/IEC 27017

An international code of practice for cloud security controls. It outlines cloud specific controls to manage security, building on the generic controls described in ISO/IEC 27002.

It's applicable to both Cloud Service Providers (CSPs) and organizations procuring cloud services. It provides support by outlining roles and responsibilities for both parties, ensuring all cloud security concerns are addressed and clearly owned.

Having ISO/IEC 27017 controls in place is especially important when you procure cloud services that form part of a service you sell to clients.

BSI provides top quality training to ensure you maximize the benefits of ISO/IEC 27017 and we also provide certification* services.

Top tip

Do you know your responsibilities when providing or procuring cloud services? It is likely all providers using ISO/IEC 27017 will have outlined and communicated responsibilities of both parties. Make sure you are aware of what you have committed to so you understand your responsibility and liability.

ISO/IEC 27018

An international code of practice for Personally Identifiable Information (PII) on public clouds. It builds on the general controls described in ISO/IEC 27002 and is appropriate for any organization that processes PII.

This is particularly important considering the changing privacy landscape and focus on protecting sensitive personal data.

BSI provides top quality training to ensure you maximize the benefits of ISO/IEC 27018 and we also provide certification* services.

CSA STAR

This is a framework based on a control set owned and created by the Cloud Security Alliance (CSA), a global industry body pioneering research and development in cloud security. BSI worked closely with CSA to develop CSA STAR's certification criteria to ensure it remains an independently verified framework for cloud security. CSA STAR contains a management capability (maturity model) to help organizations drive continual improvement.

The controls are mapped to a number of other standards making it a useful tool for organizations to review their compliance against a wide range of cloud-based standards and industry best practices. It's regularly reviewed by the CSA to ensure it remains up-to-date with industry best practice.

It's appropriate for organizations using or offering cloud services who want to demonstrate they are up-to-date with emerging best practice and gain the internal benefits of being audited against a maturity model to help steer improvements. It's widely adopted by industry-leading cloud providers and other organizations that have a dedicated focus on cloud services, enabling greater agility and resources to regularly adapt.

BSI provides top quality training to ensure you maximize the benefits of CSA STAR and we also provide certification* services.

What is a maturity model?

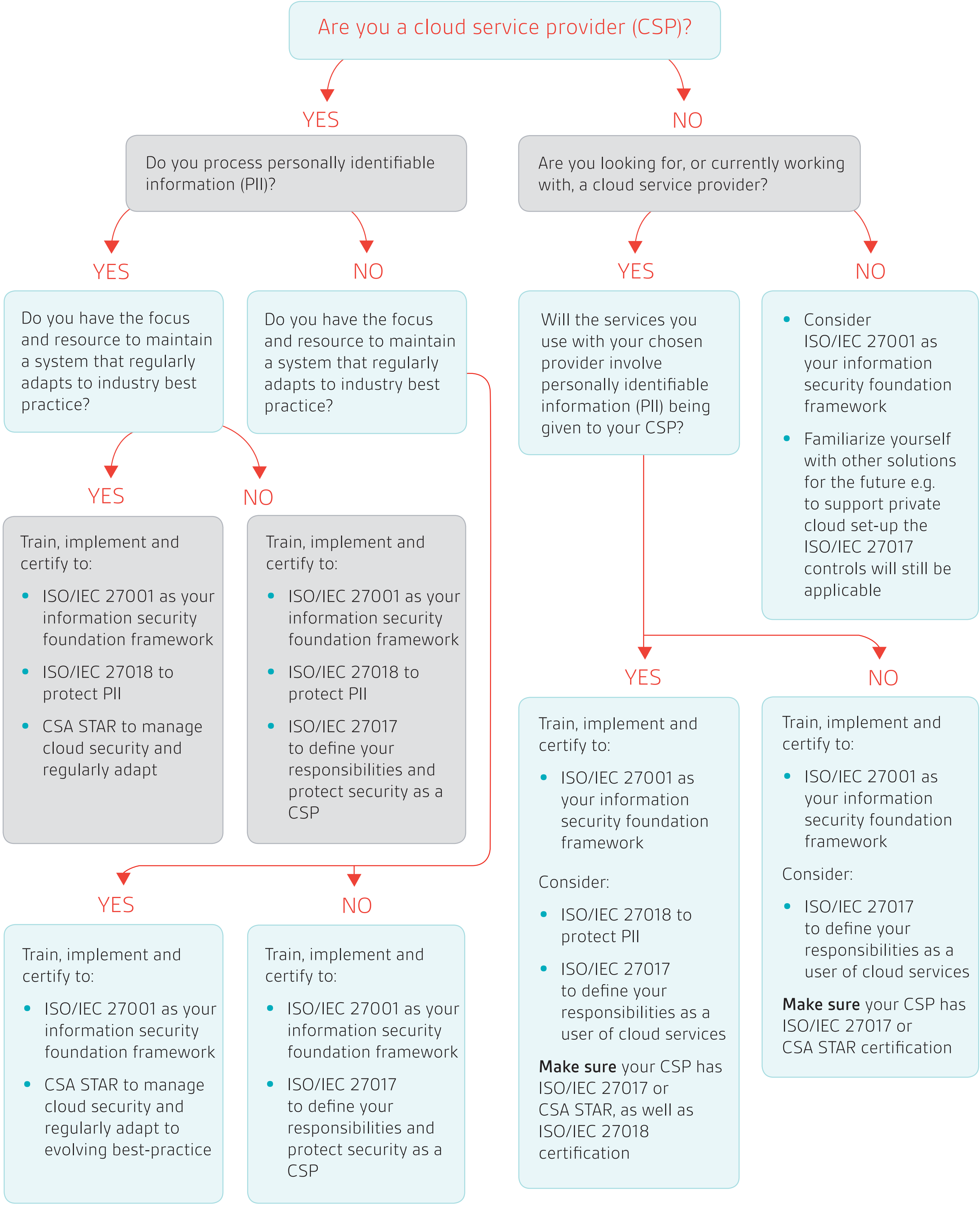
A benchmark model for managing and analyzing the performance of the cloud services you deliver. This model is regularly updated to reflect changing industry best-practice.

*You will need certification to ISO/IEC 27001 to be able to get certification to this product.

Where should I start with cloud security?

This decision tree will help you determine which solution will best meet your organizational needs.

Our training courses can help you learn about the standards and obtain the knowledge to implement and audit a system. With certification you can demonstrate your commitment to cloud security and on-going improvements.



Are you a cloud service provider (CSP)?

YES

Do you process personally identifiable information (PII)?

YES

Do you have the focus and resource to maintain a system that regularly adapts to industry best practice?

YES

Train, implement and certify to:

- ISO/IEC 27001 as your information security foundation framework
- ISO/IEC 27018 to protect PII
- CSA STAR to manage cloud security and regularly adapt

NO

Train, implement and certify to:

- ISO/IEC 27001 as your information security foundation framework
- ISO/IEC 27018 to protect PII
- ISO/IEC 27017 to define your responsibilities and protect security as a CSP

NO

Do you have the focus and resource to maintain a system that regularly adapts to industry best practice?

YES

Train, implement and certify to:

- ISO/IEC 27001 as your information security foundation framework
- CSA STAR to manage cloud security and regularly adapt to evolving best-practice

NO

Train, implement and certify to:

- ISO/IEC 27001 as your information security foundation framework
- ISO/IEC 27017 to define your responsibilities and protect security as a CSP

NO

Are you looking for, or currently working with, a cloud service provider?

YES

Will the services you use with your chosen provider involve personally identifiable information (PII) being given to your CSP?

YES

Train, implement and certify to:

- ISO/IEC 27001 as your information security foundation framework

Consider:

- ISO/IEC 27018 to protect PII
- ISO/IEC 27017 to define your responsibilities as a user of cloud services

Make sure your CSP has ISO/IEC 27017 or CSA STAR, as well as ISO/IEC 27018 certification

NO

Train, implement and certify to:

- ISO/IEC 27001 as your information security foundation framework

Consider:

- ISO/IEC 27017 to define your responsibilities as a user of cloud services

Make sure your CSP has ISO/IEC 27017 or CSA STAR certification

NO

- Consider ISO/IEC 27001 as your information security foundation framework
- Familiarize yourself with other solutions for the future e.g. to support private cloud set-up the ISO/IEC 27017 controls will still be applicable

While our decision tree gives you a good indication into what to consider, we are seeing clients certify to the full suite of standards to embed a culture of best practice that reassures users and builds confidence in their cloud security.

Here are some of the great benefits experienced by clients:

"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, Trust and Transparency Senior Director of Microsoft

ISO/IEC 27001 and CSA STAR certifications enable Cirrity to better compete with the world's largest cloud service providers.

"You are not going to find companies with a business model like ours that have invested this much in security and compliance, so that is a very big differentiator."

Dan Timko, President and Chief Technical Officer, Cirrity

"We work exclusively with BSI, the undisputed global leader in cloud security certification, on our full suite of security standards, including CSA STAR Certification, ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018 and Kitemark for Secure Digital Transactions. While BSI's superior reputation already delivers immense confidence to our customers, their true value lies in having the best expert auditors in industry who can push us to the limits, allowing us to discover our own weaknesses and continuously improve our protection of customer data."

Ronald Tse, Founder of Ribose – the world's only CSA triple-assured cloud service provider

Why BSI?

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 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 centers 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 which help facilitate this process.

To find out more visit:
bsigroup.com/en-US

bsi.

bsigroup.com/en-us