# Worried about cloud security?

Many business and governments around the world are increasingly moving more of their computing workloads over to cloud-based technologies, including commercial public clouds.

In the early days of public cloud computing, concerns were often raised about how secure these platforms really were, especially after some well-publicized breaches that were widely reported.

However, these days, many are finding that a well-chosen public cloud service is often far more secure than their previous on-premises or traditionally hosted computing platforms.

So perhaps it's time to look again at past worries and see how businesses and governments are addressing those security concerns today, with most especially using international standards that are specifically designed for the age of cloud computing.

## What is cloud computing?

If you are unclear about what 'cloud computing' means, and its implications, your first stop should be to get a copy of BS ISO/IEC 17788, which is available as a free download. This gives the official definition of cloud computing and some related terms, along with a brief explanation of them. A 'sequel' standard is being developed and will be published as BS ISO/IEC 22123 in due course. This builds on BS ISO/IEC 17788 and provides further guidance on what it all means, including ways to verify that a service marketed as a 'cloud service' really meets the definition and requirements.

A companion standard to BS ISO/IEC 17788 is BS ISO/IEC 17789, which describes a generic reference architecture for cloud computing and shows where certain elements such as security fit into the bigger picture.

## How do we keep cloud computing secure?

Cloud computing is a complex computing environment, not only as technology but also all the 'people' processes that need to be in place to use it correctly and securely.

BS ISO/IEC have developed a well-regarded Information Security Management System (ISMS) described in a number of standards in the BS ISO/IEC 27000 series. These include the following:

- BS ISO/IEC 27000 provides an overview of ISMSs
- BS ISO/IEC 27001 specifies the requirements for establishing, implementing, maintaining and continually improving an ISMS within the context of the organization. BS ISO/IEC 27001 is the core standard against which an organization can seek certification of its approach by an independent auditor

- BS ISO/IEC 27002 gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls, taking into consideration the organization's information security risk environment(s)
- BS ISO/IEC 27017 provides a code of practice and a set of controls, based on BS ISO/IEC 27002, that can be implemented to secure a cloud service

The whole process is based on risk management. BS ISO/IEC 27001 and BS ISO/IEC 27002 are used to identify the risks that need to be addressed. Controls are then identified that can be used for treatment of these risks. Those controls are then implemented either as technology or processes for people to follow. The risk analysis and the implementation of the controls can then be independently audited and (once approved by the auditor) certified as conforming to the ISMS standards.

## 24 × 7 security

A major advantage in moving to a cloud-based approach to information technology (IT) is in the scale of the security infrastructure of the reputable public cloud service providers (CSPs). The biggest CSPs have large teams of security professionals working around the clock and around the world to keep their systems safe. Their business relies on customer trust, so they spend billions of dollars on security measures.

CSPs take responsibility for perimeter security such as firewalls for their networks and data centres. They also ensure their systems are up to date with security patches and that vulnerabilities are identified rapidly and addressed worldwide.

In addition, CSPs do active research to penetrate botnets and similar IT tools of organized crime and employ analytic and predictive technologies such as artificial intelligence to anticipate security threats ahead of time and to deal with them proactively.

This level of security management is far beyond the resources of all but the very largest multinational corporations, and indeed beyond the means of many nation states.

It's also worth noting that moving to a cloud service for IT removes or greatly reduces one of the most insidious and dangerous threats to corporate security, the 'insider attack' from either a disgruntled employee or a deliberate industrial spy or saboteur with access to the equipment. Using a public cloud service puts the physical servers beyond the reach of any employee, and cloud service data centres have very high levels of physical security, audit logging and personnel vetting to prevent access by unauthorized persons.

## Moving from perimeter security to role-based security

A key aspect of moving to a secure cloud-based approach is to recognize that traditional perimeter-based security is no longer sufficient, if it ever was. At one time it was common for all the computing of enterprises to be carried out on their own servers and other computers, manned by their own staff, in their own building. As such, the main concern was to have good firewalls to keep outsiders (and malware) away from the data and services, but there were few barriers to the use of data within the organization itself.

As such, moving to a cloud-based approach brings to light the need to think more about who should be able to do what. In the modern world, giving all employees access to everything they might ever want to see has become unacceptable. It is now recognized that one of the biggest security threats to an organization is its own workforce, whether due to malice, carelessness or ignorance. A disgruntled employee can pull a vast amount of data from a server onto a USB drive or inject malware into a server. Users can become careless with passwords and other credentials. Some users may do things that seem logical to them, but in the process expose the organization to security risks.

In a cloud environment it becomes necessary to assign users to specific roles and to configure the cloud service to enable what they need while blocking what they don't. Doing this correctly and making good use of the advanced credentials and permissions provided by the cloud service is bound to lead to a more secure working environment.

There is also a clear division of responsibility between the CSP and the cloud service customer (CSC) organization. The CSP will take care of securing the hardware and, very often, also the operating systems, platform software and even applications that are being used. The big CSPs have huge teams of security experts working around the clock and around the world, not just in responding to outside threats and addressing them but also in predicting where new threats might arise and working to block them before they impact the systems. This level of security response is beyond the capabilities of all but the biggest governments and enterprises, and even they would rather not have to deal with it themselves. The CSC has to remain responsible for assigning employees to the right roles and ensuring they have only the permissions they need to do their job and ensuring those permissions are revoked when no longer needed. The CSC also needs to choose and enforce appropriate policies for handling of login credentials, and so on.

## Protecting data in the cloud

Once your organization's data moves to the cloud, the role of the cloud security functions is threefold, often abbreviated as CIA:

- Confidentiality – to ensure that the data is only made available to those who are authorized to have it, and in appropriate ways. For example, it is extremely unlikely that an employee would have any real business need to download a whole database, such as a large list of personally identifiable information (PII) pertaining to customers, employees or other data subjects
- Integrity – to ensure that the data cannot be changed except as authorized and is resistant to being corrupted
- Availability – to ensure that those people and processes who need to access the data can always do so

These three things are often related, but not always. For example, student exam results might not be kept especially confidential or available, but integrity is essential so that grades cannot be adjusted without authorization.

## Not all data is the same

Another essential aspect of cloud computing is the need to correctly categorize the data that is being held.

Some data is vital to a business and is worth considerable expense to keep protected and secret with very limited access by employees. Examples of this could include new patents being developed, upcoming advertising campaigns, financial and acquisition plans and confidential reports.

Other data must be kept secure for regulatory reasons, such as sensitive personal information, medical information and government secrets.

However, there is also a lot of other data that doesn't really need expensive confidentiality protection. Routine server activity logs, old publications, historical financial data, a history of the organization, building temperature logs, the latest menu for the cafeteria – none of those would be a concern if it leaked out, but it might often still have high value that justifies the protection of its integrity and/or availability. You wouldn't want the public history page of your organization changed by malicious individuals, even though it is very public information.

One tool that is very valuable in categorizing data is BS ISO/IEC 19944. This provides a common taxonomy of cloud service data (though it could also be used for non-cloud purposes).

This distinguishes the data held in a cloud service into

- Cloud Service Customer content, data that is submitted or created by CSCs themselves;
- Cloud Service Provider data, which the CSP needs to run the service and of no interest to CSCs;
- derived data, things that the CSP can observe from the CSC's use of the cloud service; and
- account data, things pertaining to a CSC's business relationship with the CSP.

The taxonomy then breaks these categories down further into subcategories, especially in the case of derived data. For example, you can use BS ISO/IEC 19944 to identify end user–identifiable telemetry information as a specific subcategory of derived data.

BS ISO/IEC 19944 then provides a standard structure for making statements about how data will be used by the CSP. Such statements can be included in legal service agreements, so the CSC knows in advance how its data will be handled in the cloud. So, it is possible for CSPs to use BS ISO/IEC19944 to make a declaration that they will use end user–identifiable telemetry data for making improvements to their service, but they won't share it with other parties. Using BS ISO/IEC 19944 like this ensures transparency since both the CSC and CSP know exactly what the statement covers and what it means. It is also relatively easy to translate this statement into another language for an overseas market.

## Confidentiality and classification

Much of the data of an organization will be confidential, and you will want to ensure that this can only be accessed by the right people and processes. So, in addition to the categorization of data based on BS ISO/IEC 19944, you may also want to implement a classification scheme to determine which data is of special value to the organization and to codify the rules for who can handle it and what they can do with it.

### Confidentiality versus privacy

It's important to understand that confidentiality is a more general term than privacy. Privacy refers to the privacy of individual human beings, not corporations, governments or other organizations. So, we use the general term confidentiality to cover all the multitude of things that need to be kept secret from the world outside the company. A subset of these will be matters of privacy, but many (such as a new engine design or plans for an acquisition) will not have any privacy implications.

### Classification

We're all familiar with the old spy stories where people are trying to steal 'top secret' plans or documents. Top secret in such stories is a fictional version of a level of classification.

Each organization (or indeed national government) will need to define its own data classification system, and this will usually be based on the value of the data to the organization. The value need not be financial in nature.

A classification system will typically have multiple levels, with progressively tighter rules on how data in that classification is to be kept and handled.

For example, a company might choose to define four levels of classification as

- public;
- low business impact (LBI);
- medium business impact (MBI); and
- high business impact (HBI).

They would then define what criteria would be used to decide the classification for any given data object. For example, it may be decided that data containing PII would always be classified as MBI or higher.

The system policy would then define labelling and handling rules for each classification, for example, deciding that LBI and above can never be shared using social media and that MBI and above can only be stored in storage locations approved by the IT department, while HBI must be stored on company-controlled IT systems or company-controlled cloud service tenants and only be accessible by individually authorized company employees.

Note that classification rules would also typically have specific requirements around both integrity and availability requirements; it isn't enough to think only of the confidentiality aspect of the CIA triangle. BS 10010 (Information classification, marking and handling) can help with setting up such a classification system, though it focuses on confidentiality in detail, and less so on integrity and availability.

## Privacy

As already noted, privacy refers to the correct handling of data that describes individual human beings (the 'data subjects'), whether they are employees, customers, friends of customers or others. The term 'data protection' is often used almost synonymously with data privacy in the information and communications technology (ICT) world.

Data protection law has been around for decades in many countries (often led by the UK), and this has long since been reflected in ICT system requirements. Some of these laws and regulations still make sense as the world moves to cloud computing, but there are new opportunities and new regulations that have brought all of this to a much higher level of scrutiny than ever before.

Social media networks, one of the more visible applications of cloud computing, trade on the basis of targeted advertising, by convincing people to give up private information in exchange for 'free' social network services. This has gradually raised various social concerns including privacy violations, fake news scandals, cyberbullying, use by political extremists and others. There is a danger that more constructive uses of cloud computing can be tarnished by these negative associations.

In addition, the European Union's (EU's) adoption in 2018 of the General Data Protection Regulation (GDPR) has raised the profile of both security and privacy within those organizations that do business either in or with the citizens of the EU. The very heavy penalties for breach of the GDPR have focused the minds of CEOs around the world. The gradual adoption of very similar or even 'GDPR+' laws in non-EU countries such as Switzerland, Australia, New Zealand and others (now including the US State of California) has also scared those CEOs who didn't feel worried about an EU-specific law that didn't seem to apply to them. Several large multinational corporations (such as Microsoft) are now moving to a global approach that meets or exceeds the GDPR and similar requirements worldwide, so they don't have to consider differences in privacy regimes.

The original cloud privacy standard BS ISO/IEC 27018 provides a code of practice and a set of technical and organizational measures known as 'controls' specific to handling PII in a cloud service. This has been widely adopted by cloud service providers, but it doesn't cover everything that a GDPR-like regulation is going to require.

Therefore, the international standards community has been working on a successor to BS ISO/IEC 27018 that goes further and addresses more of the legal concerns. BS ISO/IEC 27552 (Security techniques — Extension to BS ISO/IEC 27001 and BS ISO/IEC 27002 for privacy information management — Requirements and guidelines) is currently in development and colloquially known as 'PIMS' for Privacy Information Management System. PIMS will extend the ISMS mentioned earlier in some ways, as well as introducing privacy-specific controls. This helps an organization consider both security and privacy in combination.

PIMS provides a code of practice and a wider set of controls for handling personal information and, unlike BS ISO/IEC27018, it isn't limited in scope to cloud computing, nor is it limited to cloud service providers. Rather it can be for used for both cloud and non-cloud ICT

systems and even for non-IT systems such as paper files kept about people. It can be used by both CSPs and CSCs for themselves and to evaluate their supply chain.

The controls that PIMS defines are specifically designed to cover as many of the GDPR and similar legal obligations in a structured and implementable fashion. Following the code of practice and controls provided in PIMS gives a head start on following the law correctly. Further, it will be possible to obtain independent certification against PIMS (either as a cloud service provider or as a CSC).

While obtaining certification against the PIMS standard won't guarantee legal immunity from breaches of the GDPR or similar regulations, it will provide objective evidence that the organization is following industry best practices, and therefore is making a valid attempt to take reasonable care and act in good faith with respect to the law. These can go quite some way towards addressing the regulator's concerns, though of course the regulator will always eventually make its own evaluation.

It seems reasonable to expect that, in time, certification against PIMS will become the 'best practice' for all those organizations handling personal information and that such organizations will come to expect PIMS certification from their supply chain as well, no matter where they are based or do business.

At the time of writing, PIMS is expected to be published in 2019.

## Conclusions

In an age where corporate information security has become a headline issue, and where new privacy regulations are raising the expectations of both regulators and customers, both cloud computing services and the international standards that have been developed to support them are becoming increasingly attractive to businesses and to governments and government agencies.

Cloud security is a broad subject with many moving parts, but there are tools available in the international standards that can help in scoping the problem and making the best strategic decisions.

Moving from on-premises or traditionally hosted ICT systems to a large public cloud can greatly simplify security issues, especially if the public cloud service has implemented the relevant security standards mentioned earlier.

For more information about cloud computing standards Visit:
**bsigroup.com/cloudsecurity-uk**

## Annex

### What is the national standards body?

BSI is the UK National Standards Body (NSB) and was the first NSB. We represent UK's economic and social interests across all European and international standards organizations and are involved in the development of business information solutions for British organizations of all sizes and sectors.

Our role is to help improve the quality and safety of products, services and systems by enabling the creation of standards and encouraging their use.

We publish over 2,700 standards annually, underpinned by a collaborative approach, engaging with industry experts, government bodies, trade associations, businesses of all sizes and consumers to develop standards that reflect good business practice.

### Who are the ISO, IEC and JTC 1?

The ISO is the International Organization for Standardization, a global organization representing the NSBs within most countries around the world, covering standards from business practices and quality control to building materials and making tea.

The IEC is the International Electrotechnical Consortium and focuses on standards for the use and applications of electricity, from power generation and distribution to standard connectors for consumer products.

JTC 1 is a Joint Technical Committee set up between the ISO and IEC to develop standards for ICT. JTC 1 has various subcommittees (SCs) that develop standards in fields such as cloud computing (SC 38), information security and cybersecurity (SC 27), IT governance (SC 40), Internet of Things (SC 41), artificial Intelligence (SC 42) and many others.

### How are international standards developed?

Participation in these organizations is limited to subject matter experts appointed by their respective NSB. The experts may be drawn from academia, government, industry organizations and enterprises, small businesses or even private individuals as each NSB considers appropriate for each activity.

All international standards are developed by consensus between often large groups of such experts, and they go through a rigorous process of working drafts, committee drafts and, eventually, formal approval ballots, during which each involved NSB is able to make comments and to vote on final approval.

Author

**Mark Jeffrey, Microsoft – Technical Diplomat, Cloud Computing**

Mark Jeffrey has been in telecom engineering since 1983 and he started working on residential broadband concepts in 1989. In recent years, he has been a leading technical diplomat for Microsoft, working with several standards and policy organizations, including BSI. Mark Jeffrey is Vice Chairman of BSI's national committee on Cloud Computing, IST/38; this is the committee responsible for the UK input into ISO/IEC SC38, which undertakes international standards in Cloud Computing and Distributed Platforms. Mark represents BSI internationally in ISO/IEC SC38, as part of the UK delegation. Mark has a personal interest in the areas of overlap between cloud-based services, telecommunications and broadcasting.