How standards can help your business use cloud services and related technologies

Standards can be useful tools in business of all sizes; this article looks at how they can be used in your business when building or employing cloud services and related technologies, such as big data, the Internet of Things (IoT) and machine learning.

Evidence of compliance

Modern businesses face compliance[1] in many different areas, including laws, regulations, contracts, internal policies and customer requirements. When building or using cloud services, businesses will typically consider relevant privacy and data protection regulations first; however, other obligations should also be considered, such as copyright, public safety, the accessibility of the services and national (human) languages that must be supported.

[1]Please note, for the purposes of this article, there is a difference between 'compliance' and 'conformance'; a business must 'comply' with a legal obligation, such as a law, regulation or a contract; however, a business might choose to 'conform' to a standard, which is not a law, regulation or contract. Certification is when organizations have conformance to a standard 'certified' by a recognized independent organization (typically an auditor who specializes in such things). The auditor will examine the situation in detail, verify that all the mandatory requirements are being met and hopefully issue a certificate, which can then be used in making claims. This process often calls for regular follow-up checks to ensure that conformance is being maintained to the same original requirements.

Compliance with the law and regulations

In a world of modern technology, with new business models, changes in customer relationships and the emergence of new devices, apps and cloud services, it is not always easy for businesses to determine which laws or regulations apply to them, particularly when making a judgement regarding new innovations and/or business practices. If the law or regulation requires that the business takes 'reasonable measures', then using an international standard in the area could provide evidence that the business is taking a reasonable approach, in line with recognized industry best practices.

For example, using BS ISO/IEC 27552 may provide evidence that a business manages the personal information of its customers effectively. In this instance, certification could be used to serve as independent verification that businesses have effectively implemented the process and controls specified in the standard. This may act as evidence that reasonable care was taken (especially in common-law countries) and the organization was acting in good faith (especially in civil-law countries) to follow the relevant law or regulation.

Compliance with contracts and customer requirements

Writing and negotiating detailed system requirements and descriptions into customer contracts can often be a complex and expensive process, in which customers want reassurance that what they expect is delivered to them. For example, a contract may use the term 'cloud computing' without a definition and customers may be uncertain as to what they are signing up for, particularly as the term 'cloud' may simply be the rebranding of an old service.

This sort of confusion could result in a lack of trust; to overcome this, reference to standards maybe written in the contract, rather than having everything written out explicitly. For example, noting the definition of cloud as 'cloud computing as defined in BS ISO/IEC 17788' both removes the ambiguity and encourages transparency; it also allows the customer to make like-for-like product comparisons with greater ease. Please note, in these circumstances, the actions of third parties might have the effect of making the application of a standard a commercial necessity, but BSI has no control over these actions and is not a party to them.

Furthermore, while writing contract terms that describe how the customer's data will be used, which is necessary under some data protection and privacy laws, it can be helpful to use a standard such as BS ISO/IEC 19944 (Information technology — Cloud computing — Cloud services and devices: Data flow, data categories and data use). This helps identify which categories of data are being referred to and structure clear statements about how that data is going to be used. Following this approach helps ensure that both the cloud service provider and the customer have a clear understanding of what is intended.

Governance and management systems

Businesses often have many processes, which must be followed by the people involved in their management. It is best practice to document these processes. There might be a legal obligation to do this, such as in human resource procedures; however, there is also value in having clear responsibilities, procedures and records of what has happened and why, which can then be used for future reference.

Governance

Senior officers, typically, make strategic business decisions (including on governance), which are translated into policies or actions that can be followed by management and employees; it is advisable to carefully document such governance decisions. Some organizations, particularly newer businesses and those under new management, may overlook important issues or fail to keep records, which they later need.

International standards are available that describe practices for good governance, both for organizations and for specific business areas within them; for example, BS ISO/IEC 38505 (Information technology — Governance of IT — Governance of data — Part 1: Application of BS ISO/IEC 38500 to the governance of data) describes a system for managing the governance of data, summarized in Figure 1.

Using an international standard for governance helps businesses in making decisions, by providing a framework for ensuring relevant issues are considered and documented. It may also assist in identifying the necessary outputs from the governance process, which can then be used to manage the implementation of those decisions. The documentation produced for this can then also be used in evidence as already described in Figure 1, to show both due diligence and good faith on the part of the business.

Quality-based management systems

A quality-based management system is one where the intent is to improve the product or process by ensuring appropriate levels of testing, validation, feedback and continuous improvement throughout the life cycle. This can improve customer satisfaction in the service or product, which may help in increasing profits, or identify waste and inefficiency, which again may help in reducing costs.

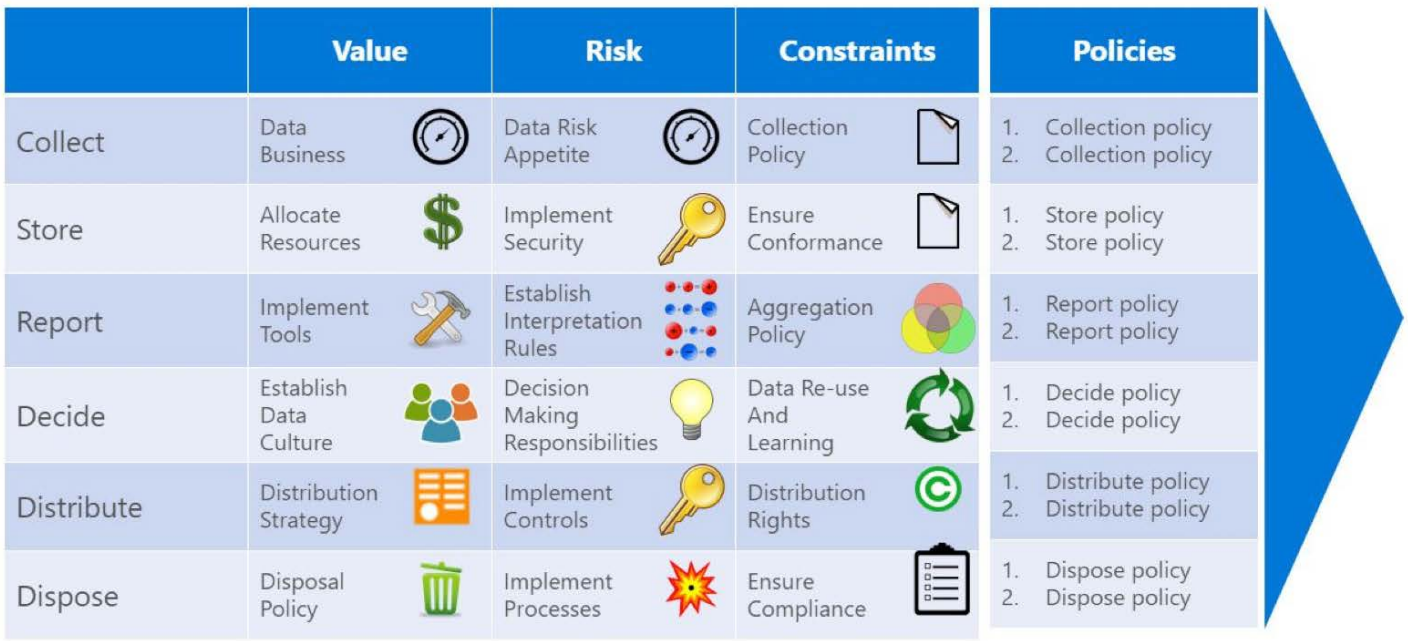
Quality-based approaches, such as Six Sigma, are generally good for dealing with relatively well-known factors or at least factors that can be reasonably anticipated, such as usability, software bug elimination and customer feedback. Businesses can resolve such issues by improvement of their own design, processes, software, and so on. A common approach to quality can be taken across almost any kind of business, with little need to customize for specific unique circumstances.

It is clear that quality-based management systems are largely reactive to things that are observed in testing or in service and therefore not generally used for planning for things that might occur in the future. For this, we may need risk-based management systems.

Risk-based management systems

A risk-based management system is used to prepare for known–unknown and unknown–unknown situations, such as new security threats or risks to human safety. Risk-based management systems are better for situations where a 'one-size-fits-all' approach is not suitable.

Figure 1 – Example – Governance of data.



In a risk-based management system, such as the well-known BS ISO/IEC 27000 series of standards for an Information Security Management System (ISMS), the approach is to identify as many risks as possible and to plan (in advance) for ways and means to eliminate or mitigate each of them, should they occur.

In many cases, the approach is to identify 'controls', which can be implemented to avoid or mitigate each specific identified risk. The BS ISO/IEC 27000 series includes 'codes of conduct' including predefined sets of candidate controls, both general (BS ISO/IEC 27002) and specific to particular concerns. A code of conduct is a formal set of behaviours and requirements that can be validated and certified by an independent auditor. For example, BS ISO/IEC 27017 has information security controls for cloud services, while BS ISO/IEC 27018 provides a code of conduct for handling Personally Identifiable Information (PII).

The upcoming standard 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 intended to provide controls that can be implemented and used to support regulatory compliance against new legal data privacy requirements, without being specific to any given jurisdiction or set of laws.

In practice, conforming to the ISMS standards means that the business can demonstrate that it has identified and analysed its own set of applicable risks, has chosen which controls are needed based on that analysis, explained why other controls are not needed and has then implemented the chosen controls according to the applicable code of conduct. Documenting this could provide evidence supporting regulatory compliance.

Conclusions

International standards have a valuable role to play in today's business world, especially in the fast-moving realm of information and communications technology and cloud services.

Standards can support businesses in complying with regulations and demonstrate best practices according to industry norms. Standards can also help structure and document decision-making in businesses. Finally, standards can help businesses maintain the quality of products and services to customers, can help anticipate and mitigate both known issues and unknown risks and can help ensure that processes are complete, repeatable and sufficiently documented.

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.