Driving Strategic Cloud Adoption

Whitepaper

bsi.

...making excellence a habit.™

Driving Strategic Cloud Adoption

Table of Contents:

Executive Summary

Cloud computing is among the most important advances in information technology (IT) to occur over the past few decades. While cost reduction was the original reason organizations adopted the cloud, recent surveys, including KPMG's 2014 Cloud Survey Report,[1] show that companies are adopting cloud technology to transform their business, to enact large-scale change and achieve customer-driven results. (KPMG, 2014)

Cloud computing, however, brings with it some unique challenges and opportunities. When it comes to selecting a cloud service provider, cost is now a lesser concern than other factors—namely, cyber security and data privacy. Information security is no longer an issue that concerns only IT and security professionals; the impact has extended to the C-suite and boardroom.[2] (PWC, 2015)

Organizations increasingly expect cloud service providers to show capabilities to fully protect information assets in a cloud environment.

The Cloud Security Alliance (CSA) STAR Certification is a rigorous independent, third-party assessment of the security of a cloud service provider. This technology-neutral certification leverages the requirements of the ISO/IEC 27001 management system standard with the CSA Cloud Controls Matrix (CCM), which is a specified set of criteria that measures the capability levels of the cloud service. It includes a unique maturity model, designed to be broadly in line with the maturity models in COBIT,[3] the Capability Maturity Model Integration (CMMI) and ISO 15504 (Software Process Improvement and Capability Determination—SPICE). The CCM also draws on the management principles found in ISO 9004.[4]

> "All businesses, no matter how advanced in their cybersecurity development, must achieve mastery of the foundational requirements of cybersecurity".
>
> **Information Security Survey, Ernst & Young**

CSA STAR Certification evaluates the efficiency of an organization's Information Security Management System (ISMS) and ensures the scope, processes and objectives are "Fit for Purpose." It helps cloud service providers prioritize areas for improvement and leads them towards business excellence.

The CSA STAR Certification perspective is one of prevention, instead of damage control, and therefore adds a great deal of value to your security and management system. It provides detailed metrics that allow you to make the best possible decisions. In addition, it provides a method for assessing your company's performance against long-term sustainability and risks, ensuring it is service level agreement (SLA)-driven, as well as allowing senior management to measure improvement year over year.

[1] http://www.ey.com/GL/en/Services/Advisory/EY-global-information-security-survey-2014-activate

[2] http://www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml

[3] The Control Objectives for Information and related Technology (COBIT) is a set of best practices (framework) for information technology.

[4] Managing for the sustained success of an organization

What Concerns Cloud Users About Cloud Based Services

CIOs and CISOs have been quick to understand that cloud computing has fundamentally changed the way data are managed both internally and when dealing with customers. According to forecasts by the Forrester Research, the public cloud market is estimated to reach $191 billion by 2020 (KPMG, 2014). This reflects major opportunities inherent in the cloud, such as diminished cost, increased efficiency and greater scalability.

Organizations have spent, and inevitably will continue to spend, precious resources on IT. The cloud allows companies of all sizes to have a greater degree of control in ensuring these resources are put to their most optimal use. For example, instead of pre-purchasing expensive server space or bandwidth to accommodate for fluctuations or expected growth, the cloud will allows clients to more nimbly add or remove capacity in real-time.

Unlike a strictly in-house IT approach, the cloud can distribute loads over a variety of users, which drastically increases the efficiency of hardware and software utilization. It also breaks down switching costs, allowing you the ability to switch service providers without absorbing sunk costs. The cloud simplifies many otherwise complex processes, which allows businesses to focus on maintaining its strategic competitive advantage instead of diverting resources to maintain its servers.

Many business processes can benefit from the adoption of cloud services. The cloud is not, however, without its own unique challenges. The adoption and maintenance of rigid security standards are essential to maximize benefits of the cloud while mitigating some potentially catastrophic negative outcomes.

Gaps within the IT ecosystem have been identified that inhibit market adoption in some key industries of secure and reliable cloud services. The general consensus is that there is not a simple, cost effective way to evaluate and compare service providers' resilience, data protection capabilities and service portability.

Consider what would happen if any service provider suffered a complete meltdown or went out of business. Given that many firms do not offer in-house backup or restore capabilities without additional costs, such critical concern factors are constantly on the mind of any CIO or CISO considering cloud adoption.

Even some of the most trusted names rely significantly on third-party vendors, and thus, are vulnerable to non-recoverable data loss. There are also concerns, many of which are valid, that cloud computing leaves data more open to corruption or unauthorized access. The data must be portable and easily accessible by the users who need it most.

Ernst & Young's recent **2014 Global Information Security Survey** reported that "all businesses, no matter how advanced in their cybersecurity development, must achieve mastery of the foundational requirements of cybersecurity".[5] The survey went on to indicate that too many organizations do not currently have all foundational components of cybersecurity in place.

No single certification, regulation or other compliance regime will supplant all others in governing the future of IT. The use of multiple standards increases the risk of adding more cost and complexity to the already overloaded compliance landscape. The rise of cloud as a global computing utility creates a mandate to better harmonize compliance concerns and ensure customer focus.[6]

Unfortunately, many organizations rely heavily on trust when additional factors like validation, verification and certification are needed to ensure safety. This gap of trust mainly outlines the difficulties that cloud users face in addressing fundamental assurance issues with cloud providers, such as:

- Understanding legal compliance and contractual liabilities
- Defining and allocating responsibilities
- Enforcing accountability
- Translating requirements into cloud language/controls/checks
- Identifying means for an ex-ante analysis assessment of cloud services
- Continuous monitoring of cloud service contract execution

What Cloud Service Providers Can Do

Cloud service providers can take advantage of the growth in this market and mitigate the many concerns of their customers by implementing an appropriate security platform. While there are a variety of platforms available, most are a derivative of the internationally-recognized industry standard: ISO/IEC 27001:2013. If you have clients in government or healthcare, you may need secondary certifications, any of which fit well under the ISO/IEC 27001 umbrella.

It is important to ensure that the overall structure of your cloud security system is analyzed and meets international standards. In order to do this, consider the Cloud Security Alliance (CSA) Open Certification Framework (OCF). The OCF is an industry initiative that allows global, accredited and trusted certification of cloud service providers. It is a program for flexible, incremental and multi-layered cloud provider certification according to the control objectives of CSA's industry-leading security guidance.

[5] http://www.ey.com/Publication/vwLUAssets/EY-global-information-security-survey-2014/$FILE/EY-global-information-security-survey-2014.pdf. Page 10. Accessed 2/8/2015.

[6] The CSA Open Certification Framework is a program for flexible, incremental and multi-layered cloud provider certification according to the Cloud Security Alliance's industry leading security guidance and control objectives.

The OCF has three levels: Self-Assessment, Certification and Continuous Monitoring. Level 2, known as Standardization Testing and Reporting (STAR) Certification is currently the highest achievable level and the most rigorous. Level 3 (Continuous Monitoring) will be launched at a later date.

The Importance of Gold-standard Security Certification

In the same report, Ernst & Young laid out six of the most frequently overlooked yet critical actions that must be considered. Number one on the list? Perform a security assessment and create an implementation roadmap. The report recommends that organizations conduct a cyber-threat assessment, current state maturity assessment, target state definition, gap analysis and design of implementation roadmap, aligning with best practices such as ISO/IEC 27001 (Ernest & Young, 2014).

ISO/IEC 27001 has evolved over 18 years to become the gold standard for the industry. Indeed, many of the other certifications are actually derived from ISO/IEC 27001. Other standards, however, tend to differ from ISO/IEC 27001 in two important ways: they are not internationally-recognized, nor are they formally managed by a strong top management driven governance process.

Security standards that rely on self-assessment techniques to address checklists with only technology-driven requirements ultimately fail to engage the deeper concerns of CIOs and CISOs. Third-parties can certify to ISO/IEC 27001 and the standard has a formal holistic management system built to detect ongoing vulnerabilities, create information security controls and preempt security threats. It is risk-based, top-down driven and its assessment helps identify the controls you need to secure your information. Because it is holistic in nature, if implemented correctly, it allows for an "Implement Once, Comply Many" strategy that reduces costs and increases effectiveness. For this reason, ISO/IEC 27001 should be used as the foundation of your cloud security program. Any other industry-specific standards and frameworks should be used either to supplement it or for specific needs, such as government or healthcare contracts. The CCM can act as additional or compensatory controls to build on to your unified integrated system, rather than create islands of information.

ISO/IEC 27001 is a holistic ISMS that, when applied using good risk management discipline, can address all cloud specific risks and relevant aspects of information security. Its benefits depend on proper scope and implementation; it must be Service Level Agreement (SLA)[7] driven. To address potential challenges and opportunities in this area, we recommend the addition of the OCF valuation process.

Your clients care that cloud providers are certified; they care about the security of their sensitive information. To provide the best level of security and service, however, its implementation is equally important; it must be "Fit for Purpose." A scope that is not fit for purpose would be irrelevant when it comes to cloud services.[8] The Level 2 of the OCF, STAR Certification, uniquely looks into scope relative to service, ensuring the most meaningful certification and providing evidence of third-party approval.

Business goals are the primary driver in interpreting the maturity of system development, along with alignment to customer and contract requirements and accurate reporting. There is, however, a fundamental order of activities and basic principles that drive the logical sequence of typical improvement efforts. This order of activities is expressed in the common features and generic practices of the capability level of the OCF architecture.

An internationally-recognized standard for security and privacy is designed to foster an extensive global adoption of cloud computing by filling the gap of trust currently perceived within cloud computing services.

These are supported by eight management principles that ensure the scope and processes are Fit for Purpose and SLA-driven:

1. **Customer focus**—Current and future needs
2. **Leadership**—Establish purpose and empower people
3. **Involvement of people**—Organizational buy-in and participation at all levels
4. **Process approach**—Resources are managed as a series of interconnecting processes
5. **Systems approach to management**—Identifying, understanding and managing interrelated processes
6. **Continual improvement**—Overall performance as a permanent objective of the organization
7. **Evidence-based approach to decision making**—Effective decisions made on analysis of real data and information
8. **Mutually beneficial supplier relationships**—Enhances the ability of both organizations to run efficiently

[7] SLA complements and forms part of a service agreement. It is a means used to incorporate business strategic objectives and define the business desired results.

[8] Reference ISO 9004

How to Measure Your Security Against Competitors

Certification provides accountability through due diligence and shows Standard of Care.[9] Until certification, you cannot be sure the crucial questions have been answered:

- Are the right data and applications being protected?
- What is the measurement system and is it measuring the correct metrics?
- How is it monitored and what is the performance evaluation process?
- How does this affect the bottom line?

Yet, after certification, many cloud providers fail to adequately address security gaps discovered during the process. After all, a certification audit is just a point in time or over a set period of time. For that reason, oversights may often go unnoticed without third-party external system evaluation and continuous monitoring.

A conventional security program may note minor or "typical" opportunities, but a program designed following CSA STAR Certification principles and controls would have identified the problem within the management system beforehand.

By ensuring the right data is collected, it can avoid a great deal of security and quality problems. Due diligence by cloud service providers is accomplished by understanding the methodologies, processes, people, controls and technologies used for security, data privacy and data center operations. CSA STAR certification can provide significant synergies to showing due diligence.

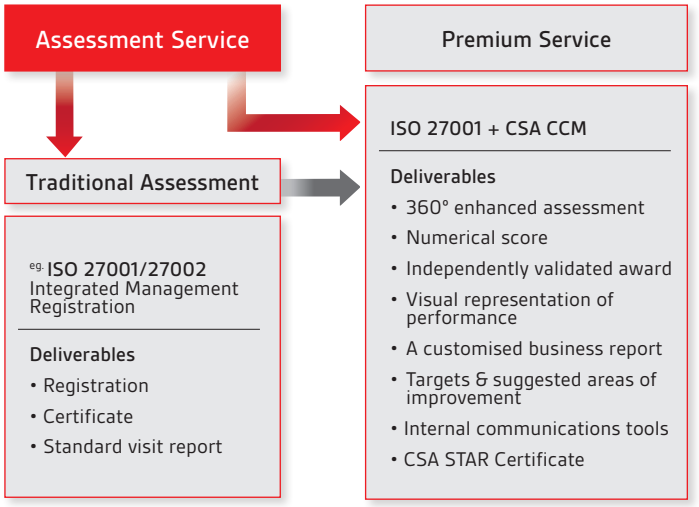
Beyond security concerns, CSA STAR evaluation can also find opportunities to deliver better service, reduce costs and improve strategic concerns. In any organization, a great deal of information is lost between the individuals who are implementing the technology and those who are setting organizational and security objectives.

By resolving this information asymmetry with proprietary techniques, the CSA STAR process can cause an organization to craft new and meaningful metrics, including but not limited to:

- trends in security risks
- percentage of third-party connections deemed secure
- percentage of business units where comprehensive business strategy is implemented
- percentage of employees that are trained and competent

Firms can use metrics to improve strategic decision making around questions of security and enterprise business improvement.

This service essentially looks at the difference between how you currently run your business and how it could be run considering security, efficiency and strategy. Through CSA STAR Certification, you will turn your investment into the greatest possible competitive advantage.



CSA STAR Certification

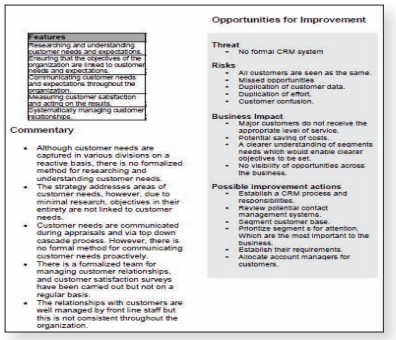
[9] The watchfulness, attention, caution and prudence that a reasonable person in the circumstances would exercise.

How to Drive Continual Process Improvement

Among the main benefits of simultaneous implementation of the ISO/IEC 27001 certification using CSA's OCF STAR Certification methodology is that the combination creates a constant feedback loop. While the ISO/IEC 27001 standard addresses the appropriate security related questions, the STAR scheme provides the solutions, as well as the means, by which to gauge how successful the current security system is by using a state-of-the-art empirical, objective and metric-based methodology.

This allows not only for you to continually monitor your security processes objectively, but also relative to your peers. According to the Ernst & Young survey, the main issues that inhibit good security governance and control stem from:

- lack of involvement from senior management
- tasks not properly resourced
- organizations are spread too thin
- effectiveness of the security process is not measured
- weak access management



Assessment Example

In short, security is still seen as a cost factor and the cost of a possible breach continues to be under-estimated. The CSA STAR Certification scheme strategically addresses these problems and provides the best practices necessary to implement ongoing security initiatives. It takes the widest possible view, bringing firms outside of their own perspective, and it looks in-depth at what your customers, clients and partners require. While this perspective is hard to secure using traditional means, CSA STAR Certification provides a sustainable and meaningful competitive advantage.

People, Processes and Technology never remain static and predictable. Staying on top of new service offerings, managing the possibility of ongoing breaches, integrating technology with new strategic business initiatives and continuing to compare the health of your security program with that of your close competitors and internal business units are essential to any organization's overall success.

Summary

In order to provide your potential clients confidence in your services, you must take steps to ensure the confidentiality, integrity, and availability of your most sensitive information.

More than ever, cloud providers need to assure customers that they have the right security certifications in place and guarantee, internally, that their systems are properly implemented. While it has been argued that the cloud providers system is more secure than the users' organizations, because it is not possible for a user to touch all points of a cloud service, more transparency is required.

Uniquely certifiable and manageable, ISO/IEC 27001, as the industry gold standard for security, must form the foundation of your information security management system. CSA STAR Certification offers the most security and strategic benefits for your management system. Leveraging these certifications can help any cloud provider ensure customer confidence, security competence and service competitiveness.

Utilizing a combination of the ISO/IEC 27001 certification and the CSA Open Certification Framework (OCF) to achieve CSA STAR Certification ensures higher integrity and greater acceptance of cloud computing.

STAR Certification was built to enhance management system standards and can provide the broadest possible view of your firm's digital security.

Implementation and certification to these standards can prevent untold damage to your firm's reputation and ensure the confidentiality, integrity, and availability of your most sensitive information. Achieving ISO/IEC 27001 certification plus CSA STAR makes an incredible statement about your organizations top-down commitment to provide the highest level of security.

To learn more about these important tools, please visit: **www.bsiamerica.com**

Bibliography

Ernest & Young. (2014). *Global Information Security Survey 2014*. E&Y.

KPMG. (2014). *2014 Cloud Survey Report -Elevating Business In The Cloud.* KPMG.

PWC. (2015). *The Global State of Information Security.* Price Waterhouse Coopers.

To learn more about ISO/IEC 27001 and Cloud Security, visit our website:

http://www.bsigroup.com/ISO-IEC-27001-us

bsi.

For more information, call 800 862 4977 or visit www.bsiamerica.com

BSI Group America Inc.
12950 Worldgate Drive, Suite 800
Herndon, VA 20170
USA
Tel: 1 800 862 4977
Fax: 1 703 437 9001
Email: inquiry.msamericas@bsigroup.com
www.bsiamerica.com

BSI Group Canada Inc.
6205B Airport Road, Suite 414
Mississauga, Ontario
L4V 1E3
Canada
Tel: 1 800 862 6752
Fax: 1 416 620 9911
inquiry.canada@bsigroup.com
www.bsigroup.ca
www.bsigroup.ca/fr

The BSI certification mark may be used on your stationery, literature and vehicles when you have successfully achieved certification and conform with applicable guidelines.

The mark shall never be applied directly on the product or service.