Strategic Cloud Adoption

The Four Steps to Safely and Strategically Leverage the Cloud

In this whitepaper, you will learn how to:

- Select the right cloud-based services
- Implement gold-standard security certifications
- Measure your security against competitors
- Drive continual process improvement

For more information, please visit www.bsiamerica.com

Table of Contents:

...making excellence a habit.™

Strategic Cloud Adoption

The Four Steps to Safely and Strategically Leverage the Cloud

Executive Summary:

Cloud computing is among the most important advances in information technology (IT) to occur in the past few decades. It is increasingly gaining prominence and attention in the world of IT; however it brings with it some unique challenges and opportunities. Ernst & Young's 2011 Global Information Security Survey of 1,700 CIOs, CISOs, CFOs, and CEOs in 52 countries reported that in the absence of clear guidance many organizations seem to be making ill-informed decisions, either moving to the cloud prematurely without appropriately considering the associated risks or avoiding it altogether. Despite these security concerns, 61% said they would be moving to cloud services (Ernst & Young's Global Information Security Survey, 2011). In order to optimize your use of these technologies, consider a four-step process that will maximize the benefits to your firm and minimize the potential security-related downside associated with cloud services.

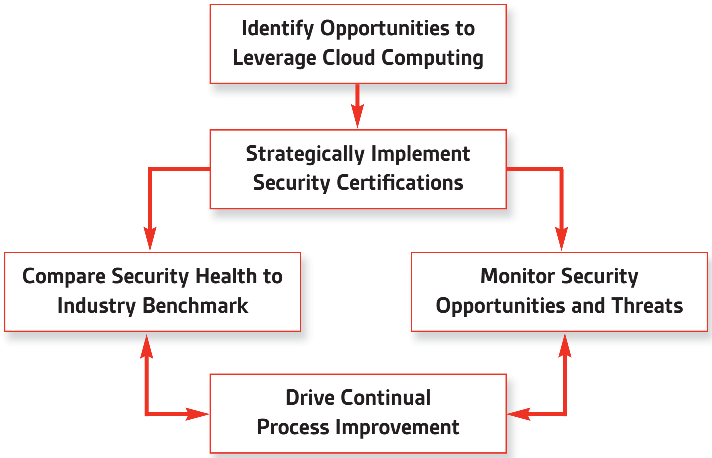

Identify Opportunities to Leverage Cloud Computing
Strategically Implement Security Certifications
Compare Security Health to Industry Benchmark
Monitor Security Opportunities and Threats
Drive Continual Process Improvement

Figure 1 – Classic Cloud Adoption

1. The first step is to **identify opportunities** by finding the right business processes that could benefit from cloud services. The cloud must be "fit for purpose", for example it can be used to simplify processes, cut costs, and provide a greater degree of scalability and flexibility in consumption of IT resources.
2. The second step is to **select and strategically implement** the most appropriate security platform. There are a variety from which to choose; however most of them are a derivative of the industry gold standard: ISO/IEC-27001:2005. You may also need secondary certifications if you have clients in government or healthcare.
3. The third step is to **take a step back** from the details of implementation and look at the overall structure of your cloud security system. One initiative that supports this activity is the Cloud Security Alliance (CSA) Open Security Framework (OCF)[1] premium service. The OCF is based on the CSA Cloud Control Matrix (CCM)[2] and a unique maturity model; designed to be broadly in line with the maturity models in COBIT[3] and the Capability Maturity Model Integration (CMMI) as well as ISO 15504 (Software Process Improvement and Capability Determination - SPICE) and draws on the management principles in ISO 9004[4].

   The OCF simultaneously evaluates security posture, makes sure your scope is "Fit for Purpose,"[5] suggests areas for improvement, and compares your organizations health to a portfolio of peers in your industry. These crucial services can prevent untold damage to your firm's reputation and ensure the confidentiality, integrity, and availability of your most sensitive information. The OCF perspective is one of prevention instead of damage control and therefore adds a great deal of value to your security and management systems. It provides detailed metrics that allow you to make the best possible decisions.
4. The fourth step, **driving continual process improvement**, is also part of the OCF. Technology never remains 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 your security health with that of your close competitors and internal business units is an essential part of any organization's overall success.

In summary, the combination of the ISO/IEC 27001 certification and OCF lends to higher integrity in and acceptance of cloud computing. It was built to enhance management system standards and can provide the broadest possible view of your firm's digital security. Together, they maximize the strategic benefit to your firm and security strength of your data, providing the additional credentials of STAR Certification (Standardized Testing and Reporting).

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

[1] 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.

[2] Cloud Controls Matrix (CCM) is specifically designed to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider.

[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

[5] Fit for Purpose is an expression that when used within the solution negotiation context, places an onus of responsibility upon the vendor to ensure that its solution is (indeed) fit for the purpose, which their client expects.

The Steps in Detail:

1. Identify Opportunities to Leverage Cloud Computing

CIOs and CISOs have been quick to understand that cloud computing has fundamentally changed the way data is managed, both internally and when dealing with customers. According to forecasts by the International Data Corporation (IDC), cloud spending will account for 25% of the year's annual IT expenditure growth and almost 33% of the growth next year. This reflects the major opportunities inherent in the cloud, such as diminished costs, increased efficiency, and greater scalability. Most industry professionals group the cloud into three general taxonomies, each with its own specific uses: Software as a Service, Infrastructure as a Service, and Platform as a Service.

Cloud Type	Description
Software as a Service (SAAS)	Most cloud computing falls under this category. It includes software programs that are hosted, accessed, and interfaced with online as opposed to on local servers or computers such as Google apps, Salesforce.com's CRM, and e-mail services.
Infrastructure as a Service (IAAS)	This is likely the second most utilized element of cloud computing. It includes the ability to access servers, storage, computers, and other hardware-related services. Examples include Dropbox, Amazon CloudFormation, and Rackspace Cloud.
Platform as a Service (PAAS)	The cloud can also make accessible a computing platform and its relevant solution stack. This is most useful in developing, testing, and deploying web applications. Examples include Amazon Electric Beanstalk, Google App Engine, and Microsoft Azure.

Figure 2 – Cloud Services

Your firm has spent, and inevitably will continue to expend, precious resources on information technology. However 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 allow you to more nimbly add or remove capacity in real-time.

Unlike a strict 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 also simplifies many otherwise complex processes, which allows your business to focus on maintaining its strategic competitive advantage instead of diverting resources to maintain its servers.

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

Gaps within the IT ecosystem have been identified that are inhibiting market adoption of secure and reliable cloud services. Consumers do not have simple, cost effective ways to evaluate and compare their providers' resilience, data protection capabilities, and service portability.

Recognizing that 1) no single certification, regulation or other compliance regime will supplant all others in governing the future of IT, and 2) the use of multiple standards increases the risk of adding more cost and complexity to the already overloaded compliance landscape, the rise of the cloud as a global compute utility[6] creates a mandate to better harmonize compliance concerns and ensure customer focus.

Unfortunately, most respondents in the pre-mentioned Ernst & Young survey 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

Almost 90% of the respondents are in favor of external certification, with nearly half (45%) saying this should be based only on an agreed-upon standard. The market need for independent verification and certification is recognized by several independent bodies. In fact, great strides forward have been made recently regarding insightful guidance on cloud certification through the development of the OCF (Ernst & Young's Global Information Security Survey, 2011).

[6] Packaging of computing resources, such as computation, storage and services, as a metered service. This model has the advantage of a low or no initial cost to acquire computer resources; instead, computational resources are essentially rented.

2. Strategically Implement Security Certifications

Consider what would happen if a 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 should be 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. And, finally, to be practical, the data must be portable as well: easily accessible by the users who need it most.

Figure 3 - STAR Certification

As such, before implementing any cloud-based solutions, savvier CIOs and CISOs look for a solid and comprehensive measure of security risk. Currently, one can find a host of general standards and frameworks including ISO/IEC 27001:2005, SOC1 and SOC2, FedRAMP, and others. What makes one standard right or wrong for you? To begin with, some standards like FedRAMP are specifically required for work with government clients. But the majority of other standards seem to serve relatively similar purposes.

Since it has evolved and grown over a 17-year period, ISO/IEC 27001 is considered the industry gold standard. Indeed, many of the other certifications are actually derivative in as much as they were created using the ISO as their reference. However, other standards tend to differ from ISO/IEC 27001 in two important ways in that they are neither internationally certifiable nor formally managed.

Security standards that rely on self-assessment techniques and addressing checklists ultimately fail to engage in the deeper concerns that CIOs and CISOs truly care about. ISO/IEC 27001 is certifiable by an accredited firm and has a formal management system to detect ongoing vulnerabilities, create information security controls, and preempt security threats. It is risk based, and its assessment helps identify the controls you need to secure your information. For this reason, ISO/IEC 27001 should be used as the foundation of your cloud security program, while simultaneously using any other industry specific standards and frameworks either to supplement it or in support of specific needs such as government or healthcare contracts. The CCM can then provide additional or compensatory controls to facilitate a unified integrated system rather than islands of information.

ISO/IEC 27001 is a holistic information security management system 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.

Clients care that cloud providers are certified; they care about the security of their sensitive information. However to provide the best level of security and service, implementation of the information security management system is equally important as it must be "Fit for Purpose." ISO/IEC 27001 plus OCF uniquely looks into scope relative to service, ensuring the most meaningful certification and providing the additional STAR Certification as evidence of 3rd party approval.

Additionally ISO/IEC 27001 measures the organization on business goals. Business goals are the primary driver in interpreting the maturity of system development and alignment with requirements of contracts and customers along with reporting reality versus expectations. But, there is 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 side of the OCF architecture.

Such a globally recognized standard for security and privacy is supposed 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 (8) management principles[8] 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

3. Monitor Opportunities & Threats and Compare Security to Industry

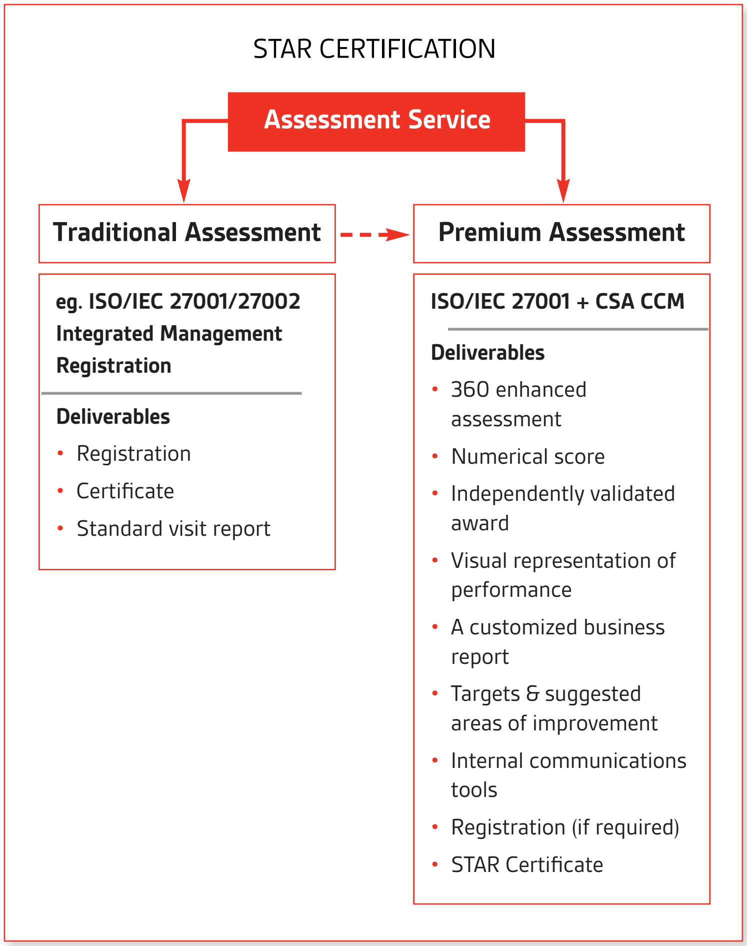
Certification provides accountability through due diligence and shows Standard of Care[9]. Until certification, one cannot be sure the crucial questions have been answered: Are the right data and applications being protected? What is the measurement system? How is it monitored? How does this affect the 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. For that reason, oversights may often go unnoticed without third-party external system valuation and continuous monitoring.

A conventional security program may note minor or "typical" opportunities, but an OCF designed program can identify 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 on cloud service providers is accomplished by understanding the methodologies, processes, people, controls, and technologies used for security, data privacy, and data center operations. Third-party assessments and certifications with the additional OCF assessment can provide significant synergies to showing due diligence.

Beyond security concerns, OCF valuation 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 OCF can 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, and percentage of employees that are trained and competent.

Not only do firms receive these important metrics that improve strategic decision making around questions of security, but they can also see how they rank compared to an industry benchmark and their top competitors. Based on this data, OCF will set targets and processes in place to drive continual improvement that align with overall strategic goals and initiatives. 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 OCF, the standard is implemented correctly, turning your investment in the cloud into the greatest possible competitive advantage.



STAR CERTIFICATION

Assessment Service

Traditional Assessment

eg. ISO/IEC 27001/27002 Integrated Management Registration

Deliverables
- Registration
- Certificate
- Standard visit report

Premium Assessment

ISO/IEC 27001 + CSA CCM

Deliverables
- 360 enhanced assessment
- Numerical score
- Independently validated award
- Visual representation of performance
- A customized business report
- Targets & suggested areas of improvement
- Internal communications tools
- Registration (if required)
- STAR Certificate

Figure 4 – STAR Process

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

4. Drive Continual Process Improvement

Among the main benefits of simultaneous implementation of the ISO/IEC 27001 certification and the OCF service is that the two create a constant feedback loop. While the ISO/IEC 27001 standard addresses the appropriate security related questions, OCF provides the solutions, as well as a 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 you to continually monitor your security objectively, but also relative to your peers. According to the Ernst & Young survey, 80% of CIOs are challenged to deliver information security initiatives for new technologies such as cloud computing and virtualization. OCF strategically addresses these problems and provides the guidance necessary to implement ongoing security initiatives. It takes the widest possible view, bringing firms outside of their own perspective, and looks in-depth at what your customers, clients, and partners require. This perspective is hard to secure using traditional means and provides a sustainable and meaningful competitive advantage.

FEATURES

- Researching and understanding customer needs and expectations.
- Ensuring that the objectives of the organization are linked to customer needs and expectations.
- Communicating customer needs and expectations throughout the organization.
- Systematically managing customer relationships.

COMMENTARY

- Although customer needs are captured in various divisions on a reactive basis, there is no formalized method for researching and understanding customer needs.
- The strategy addresses areas of customer needs, however, due to minimal research, objectives in their entirety are not linked to customer needs.
- Customer needs are communicated during appraisals and via top down cascade process. However, there is no formal method for communicating customer needs proactively.
- There is a formalized team for managing customer relationships, and customer satisfaction surveys have been carried out but not on a regular basis.
- The relationships with customers are well managed by front line staff but this is not consistent throughout the organization.

OPPORTUNITIES FOR IMPROVEMENT

Threat

- No formal CRM system.

Risks

- All customers are seen as the same.
- Missed opportunities.
- Duplication of customer data.
- Duplication of effort.
- Customer confusion.

Business Impact

- Major customers do not receive the appropriate level of service.
- Potential saving of costs.
- A clearer understanding of segments needs which would enable clearer objectives to be set.
- No visibility of opportunities across the business.

Possible improvement actions

- Establish a CRM process and responsibilities.
- Review potential contact management systems.
- Segment customer base.
- Prioritize segments for attention which are most important to the business.
- Establish their requirements.
- Allocate account managers for customers.

Figure 5 – Assessment Example

CONCLUSION

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. ISO/IEC 27001, as the industry gold standard for cloud security, being uniquely certifiable and manageable, must form the foundation of your certification standards. In order to get the most security and strategic benefits from your standard, one can also utilize the OCF. With these four steps, cloud providers are more apt to ensure customer confidence, security competence, and service competitiveness.

You can leverage the significant benefits of the cloud at the greatest benefit to your firm while minimizing its potential downsides. Achieving ISO/IEC 27001 certification plus STAR Certification makes an incredible statement about your organizations Top-Down commitment to provide the highest level of security and ultimately the peace of mind that is so much on the minds of organizations today.

References:

- IDC's IT Cloud Services Forecast 2009 – 2013. (2009). International Data Corporation. Accessed from: http://blogs.idc.com/ie/?p=543
- Ernst & Young's Global Information Security Survey. (2011). Ernst & Young Global.

BSI/USA/337/MS/0413/E

For more information, call 888-429-6178
or visit www.bsiamerica.com

BSI Group America Inc.
12110 Sunset Hills Road, Suite 200
Reston, VA 20190-5902
USA
Tel: 1 888 429 6178
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.