ISACA
Trust in, and value from, information systems

AN ISACA CLOUD VISION SERIES WHITE PAPER

SECURITY AS A SERVICE: Business Benefits With Security, Governance and Assurance Perspectives

Enterprises need to protect their assets, but they also need to be profitable to stay in business. Protecting information assets has become a priority for enterprises that need to meet compliance requirements or need to protect sensitive data. The challenge for these enterprises is implementing robust security practices while keeping investment and operational cost contained. SecaaS offers a way for enterprises to access security services that are robust, scalable and cost effective. With reward comes risk, and enterprises should consider benefits and risk when evaluating SecaaS products and providers. Above all, enterprises need to understand that they can outsource responsibility but they can't outsource accountability; therefore, enterprises should implement an assurance plan that includes assessing the services obtained from SecaaS providers. When an audit is not possible, enterprises must still obtain proof that controls used to protect enterprise information assets are working effectively.

ABOUT ISACA®

With more than 110,000 constituents in 180 countries, ISACA *(www.isaca.org)* helps business and IT leaders maximize value and manage risk related to information and technology. Founded in 1969, the nonprofit, independent ISACA is an advocate for professionals involved in information security, assurance, risk management and governance. These professionals rely on ISACA as the trusted source for information and technology knowledge, community, standards and certification. The association, which has 200 chapters worldwide, advances and validates business-critical skills and knowledge through the globally respected Certified Information Systems Auditor® (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) and Certified in Risk and Information Systems Control™ (CRISC™) credentials. ISACA also developed and continually updates COBIT®, a business framework that helps enterprises in all industries and geographies govern and manage their information and technology.

Disclaimer

ISACA has designed and created *Security as a Service: Business Benefits With Security, Governance and Assurance Perspectives* (the "work") primarily as an educational resource for governance and assurance professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, governance and assurance professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA

Phone: +1.847.253.1545

Fax: +1.847.253.1443

Email: *info@isaca.org*

Web site: *www.isaca.org*

Provide feedback:
www.isaca.org/security-as-a-service

Participate in the ISACA Knowledge Center:
www.isaca.org/knowledge-center

Follow ISACA on Twitter:
https://twitter.com/ISACANews

Join ISACA on LinkedIn:
ISACA (Official)
http://linkd.in/ISACAOfficial

Like ISACA on Facebook:
www.facebook.com/ISACAHQ

Acknowledgements

ISACA Wishes to Recognize:

Project Development Team

Patrick Hanrion,
CISM, CISSP, CNE, MCSE, Expedia, USA

Alan Mayer,
CISA, CISSP, Security Management Partners, USA

Yogendra Rajput,
India

Paras Shah,
CISA, CGEIT, CRISC, CA, Vital Interacts, Australia

Ron Speed,
CISA, CRISC, CA, Trusted Impact, Australia

Expert Reviewers

Sai K. Honig,
CISA, CIA, USA

Sami Kaukinen,
CISM, CISSP, Finland

Larry Marks,
CISA, CGEIT, CRISC, CISSP, PMP, CFE, IBM, USA

Bassil Mohammad,
CISA, CISM, CRISC, MSc, CEH, LISA, Ernst & Young Amman, Jordan

Leonard Ong,
CISA, CISM, CRISC, CPP, CFE, CISSP, PMP, Barclays Capital, Singapore

Simon Reeves,
CISA, CISSP, RBS Group, UK

Amr Ahmed Said,
CISA, CISM, CGEIT, CRISC, Nokia Siemens Networks, Egypt

Theodoros Stergiou,
Ph.D., CPMM, CCDA, CSSDS, Intracom Telecom, Greece

Ability Takuva,
CISA, Barclays Africa, South Africa

Alejandro Tinoco Zavala,
CISA, CISM, CGEIT, CRISC, Mexico

ISACA Board of Directors

Tony Hayes,
CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Queensland Government, Australia, International President

Allan Boardman,
CISA, CISM, CGEIT, CRISC, ACA, CA (SA), CISSP, Morgan Stanley, UK, Vice President

Juan Luis Carselle,
CISA, CGEIT, CRISC, RadioShack, Mexico, Vice President

Ramses Gallego,
CISM, CGEIT, CCSK, CISSP, SCPM, Six Sigma Black Belt, Dell, Spain, Vice President

Theresa Grafenstine,
CISA, CGEIT, CRISC, CGAP, CGMA, CIA, CPA, US House of Representatives, USA, Vice President

Vittal Raj,
CISA, CISM, CGEIT, CFE, CIA, CISSP, FCA, Kumar & Raj, India, Vice President

Jeff Spivey,
CRISC, CPP, PSP, Security Risk Management Inc., USA, Vice President

Marc Vael,
Ph.D., CISA, CISM, CGEIT, CRISC, CISSP, Valuendo, Belgium, Vice President

Gregory T. Grocholski,
CISA, The Dow Chemical Co., USA, Past International President

Kenneth L. Vander Wal,
CISA, CPA, Ernst & Young LLP (retired), USA, Past International President

Christos K. Dimitriadis,
Ph.D., CISA, CISM, CRISC, INTRALOT S.A., Greece, Director

Krysten McCabe,
CISA, The Home Depot, USA, Director

Jo Stewart-Rattray,
CISA, CISM, CGEIT, CRISC, CSEPS, BRM Holdich, Australia, Director

Knowledge Board

Christos K. Dimitriadis,
Ph.D., CISA, CISM, CRISC, INTRALOT S.A., Greece, Chairman

Rosemary M. Amato,
CISA, CMA, CPA, Deloitte Touche Tohmatsu Ltd., The Netherlands

Steven A. Babb,
CGEIT, CRISC, Betfair, UK

Thomas E. Borton,
CISA, CISM, CRISC, CISSP, Cost Plus, USA

Phil J. Lageschulte,
CGEIT, CPA, KPMG LLP, USA

Anthony P. Noble,
CISA, Viacom, USA

Jamie Pasfield,
CGEIT, ITIL V3, MSP, PRINCE2, Pfizer, UK

Guidance and Practices Committee

Phil J. Lageschulte,
CGEIT, CPA, KPMG LLP, USA, Chairman

John Jasinski,
CISA, CGEIT, ISO20K, ITIL Exp, SSBB, ITSMBP, USA

Yves Marcel Le Roux,
CISM, CISSP, CA Technologies, France

Aureo Monteiro Tavares Da Silva,
CISM, CGEIT, Brazil

Jotham Nyamari,
CISA, CISSP, Deloitte, USA

James Seaman,
CISM, CRISC, A. Inst. IISP, CCP, MSc, QSA, RandomStorm, UK

Gurvinder Singh,
CISA, CISM, CRISC, Australia

Siang Jun Julia Yeo,
CISA, CPA (Australia), MasterCard Asia/Pacific Pte. Ltd., Singapore

Nikolaos Zacharopoulos,
CISA, CRISC, CISSP, DeutschePost–DHL, Germany

Introduction

Information is the currency of the 21st century. Enterprises of all sizes and from all industries understand that protecting information assets is critical to their success. A security breach means more than the cost to repair vulnerable hardware or software. A security breach can result in the loss of intellectual assets vital to an enterprise's competitive advantage, loss of business due to reputation damage or huge fees associated with regulatory fines and lawsuits by third parties affected by the breach.

According to ISACA, information security "ensures that within the enterprise, information is protected against disclosure to unauthorised users (confidentiality), improper modification (integrity) and non-access when required (availability)."[1] Enterprises understand that information security is not an option, but, rather, a necessity. From small retailers that use point of sale (PoS) devices to read credit cards, to large conglomerates doing business around the world, all enterprises need to protect their information and their customers' information. A recent survey conducted by the UK government Department for Business, Innovation and Skills shows that small businesses are experiencing security incidents at a rate experienced previously only by large enterprises. The survey shows that, within a 12-month period, 93 percent of large enterprises and 87 percent of small businesses had a security breach. The average cost for a small business to address the damage caused by its worst security breach of the year was between £35K and £65K (US$56K and $105K).[2]

Many enterprises that needed to implement robust security practices while keeping costs down have outsourced specific applications and tasks to Managed Security Service Providers (MSSPs). MSSPs promise to handle sophisticated, costly and time-consuming security tasks following traditional outsourcing practices. MSSP practices usually are more rigid than cloud-based outsourcing practices, which offer elasticity and may not require an enterprise to transfer assets to the provider to support the process under contract. MSSP outsourcing is enticing to enterprises because MSSPs offer a way to access security management expertise and infrastructure resources without adding overhead costs to the enterprise.

Security as a Service (SecaaS) is the next generation of managed security services dedicated to the delivery, over the Internet, of specialized information-security services.[3]

The SecaaS model embraces all of the cloud computing characteristics ("convenient, on-demand network access to a shared pool of resources that can be rapidly provisioned and released with minimal management effort or service provider interaction").[4] Another characteristic of SecaaS is that users may have less or no control over services and tasks due to the inherent nature of cloud computing.

The terms MSSP and SecaaS are used interchangeably when discussing the practice of contracting a third party to provide security services. For the purpose of this paper, the term SecaaS will be used.

SecaaS can be delivered using the cloud model Software as a Service (SaaS), Platform as a Service (PaaS) or Infrastructure as a Service (IaaS), depending on the level of protection procured by an enterprise. Gartner Inc. forecasts that cloud-based security services will account for 10 percent of the enterprise IT security product market by 2015.[5] Infonetics Research forecasts that cloud-based security revenue will increase at a 10.8 percent compound annual growth rate (CAGR) through 2017, to reach US$9.2 billion.[6]

Some of the services offered by SecaaS providers are:

- **Identity and access management (IAM)**
- **Email security (important when implementing a secure Bring Your Own Device [BYOD] program)**
- **Antivirus and anti-malware/spyware**
- **Intrusion management (detection and prevention)**
- **Security infrastructure deployment and management**
- **Security information monitoring and event management (SIEM) (important for regulatory compliance in monitoring and reporting)**
- **Firewall integration and management**
- **Encryption**
- **Integrity monitoring**
- **Tokenization (important for Payment Card Industry Data Security Standard [PCI DSS] compliance and other privacy mandates)**
- **Web site security and Secure Sockets Layer (SSL) certificates**
- **Remote vulnerability assessment**
- **Configuration compliance assessment**
- **Application security static and dynamic analysis**
- **Internet traffic filtering**
- **Data loss management (monitoring, prevention and reporting)**
- **Security assessments**
- **Business continuity and disaster recovery**
- **Network security**

Some analysts say that the greatest benefit from using SecaaS is economic, but one could argue that, in a world where threats to information are constantly evolving, the greatest advantage is the ability to use the latest technologies to counter these threats. SecaaS levels the security playing field for enterprises of all sizes. Small businesses can now use the same tools that were affordable to only large enterprises before cloud computing became ubiquitous. Huge capital investment and specialized skills are not needed to

implement and manage some of the security solutions offered by SecaaS vendors, making these solutions affordable to businesses of all sizes.

A counterpart to the benefits of using SecaaS is the additional risk that enterprises must be willing to accept to make SecaaS a valuable solution.

Using a third party to provide critical services requires an enterprise to relinquish some control, which frees the enterprise to focus resources on core competencies but also creates a dependency on the third party to be reliable, financially resilient and sustainable. Internal controls do not disappear after contracting a SecaaS vendor; rather, controls must be updated to reflect the new environment and focus more on governance and assurance to ensure that critical services do not suffer disruptions.

The potential impact of SecaaS on the enterprise is discussed in this white paper. The paper identifies prospective business benefits, challenges and risk; presents recommended governance and risk management practices; and provides an overview of assurance considerations.

[1] ISACA, *COBIT® 5 for Information Security,* USA, 2012

[2] UK Department for Business, Innovation and Skills, "2013 Information Security Breaches Survey," *www.gov.uk/government/uploads/system/uploads/attachment_data/file/191671/bis-13-p184es-2013-information-security-breaches-survey-executive-summary.pdf*

[3] Janalta Interactive Inc., "Security as a Service (SecaaS or SaaS)," *www.techopedia.com/definition/26746/security-as-a-service-secaas-saas*

[4] Mell, Peter; Timothy Grance; US National Institute of Standards and Technology (NIST) Special Publication (SP) 800-145, The NIST Definition of Cloud Computing, NIST, USA, 2011

[5] Blevins, Brandan; "Gartner forecasts rising interest in cloud-based security services," techtarget.com, 17 April 2013, *http://searchcloudsecurity.techtarget.com/news/2240181882/Gartner-forecasts-rising-interest-in-cloud-based-security-services*

[6] Infonetics Research, "Cloud security services to top $9 billion by 2017, barring stumbling blocks," 17 October 2013, *www.infonetics.com/pr/2013/1H13-Cloud-and-CPE-Managed-Security-Services-Market-Highlights.asp*

Impact of SecaaS on the Enterprise

As with other cloud-related service offerings, SecaaS promises much—security services that are accessible to anyone, low capital costs, unbounded scale and elasticity, low-cost options for small enterprises, etc.

The need for better information security in most geographic locations and industry sectors is growing rapidly. Enterprise information security is complex, expensive and resource-constrained. In recent years, mobile computing and cloud-based IT have added to the complexity of tasks of enterprise IT organizations. As consumers, regulations and governance expectations focus increasingly on the need for adequate security, using SecaaS can become an irresistible opportunity to improve security and compliance while controlling cost.

The rapid adoption of mobile devices and cloud-based technologies among enterprises of all sizes means that security is now a critical need for all enterprises. The past decade has seen a massive democratization of IT.

SecaaS is moving information security in the same direction by reshaping how security services are offered in the marketplace.

Major corporations with substantial budgets and teams are no longer the only enterprises with access to state-of-the-art security capabilities. SecaaS enables small to medium-sized enterprises with minimal internal security capability to access the most advanced information security services.

SecaaS providers also have challenges. This new way to manage and deliver security services offers tremendous opportunities—new sales and delivery channels, access to growing global marketplaces and an eager new set of potential clients. SecaaS revenues (charging for only the services and resources that clients use) can potentially cannibalize legacy revenues, which are often based on licensing fees, implementation costs and maintenance contracts. With lower barriers to enter markets, competition is growing rapidly. There is also the inevitable commoditization of services and resulting pressure on margins. Therefore, SecaaS providers must differentiate themselves—through quality, reliability and, most importantly, trustworthiness. One distinguishing element is the level of transparency that a provider offers about its services, including its own internal security practices.

Like any innovation, SecaaS has significant disruptive potential. For example, enterprise security functions may feel threatened by external providers that offer low-cost, highly scalable services. The increasing need for services in the marketplace and the perpetual shortfall of capable security resources suggest that the net outcome will be generally positive for security professionals.

SecaaS raises the following new questions and potential issues related to governments and regulations:

- **Who is responsible for securing what?**
- **Who has access to what data?**
- **Where are important security data (audit logs, user credentials, etc.) stored and can they be accessed when needed?**
- **What are the destruction and archival procedures?**
- **What legal and jurisdictional issues do cross-border SecaaS offerings raise?**
- **What new data privacy and access management issues are raised by SecaaS?**
- **As SecaaS grows in popularity, will more regulations be created to deal specifically with some of these potential issues?**

SecaaS does not relieve an enterprise of information security responsibility. The enterprise can outsource information security services, but not accountability for security.

With or without SecaaS, an enterprise remains responsible for all of its sensitive information. Laws and regulations enforce this accountability. The enterprise must know the information and IT assets that are critical to its organization, its customers and its stakeholders and the risk that is associated with these critical assets. Without this vital understanding, there is no way for the enterprise to determine the security services that it needs and the threats that it needs protection against.

Business Benefits of SecaaS

The migration to SecaaS is driven by several factors, including a lack of skilled in-house IT security staff and the need to reduce costs and compliance regulations that must be adhered to quickly, according to Eric Ahlm, research director at Gartner.[7] Gartner predicts within the next three years that 10 percent of overall IT security enterprise product capabilities will be cloud-based.[8] The economic and operational benefits spurring this rapid transition to cloud-based SecaaS are:[9]

- **Cost—**An enterprise pays only for the services and resources it uses, as it uses them, with SecaaS. By moving security services and maintenance workloads to a cloud platform, the enterprise has the ability to instantly increase or decrease resources, depending on the immediate needs of a particular workload. Web-site vulnerability scans, security monitoring and incident response, identity access management and data encryption services are some of the security services that can be moved to the cloud, controlled, and paid for only when used. With SecaaS, very limited up-front capital investment is required for hardware and software, ongoing software licenses costs are eliminated, the need for complex technologies is limited and services can be delivered and accessed from almost anywhere in the world. Fewer servers running security applications means a smaller data center footprint. That can translate to direct savings on real estate, power and cooling and indirect savings on facilities maintenance.[10]
- **Ease of management and operations—**The SecaaS provider is responsible for the management and operation of hardware and software that is used to deliver services to the enterprise. Using a web-interface console, an enterprise can view the security environment and activities and perform the control tasks that it chooses to manage. The console alerts the enterprise of security incidents that require its attention and provides auditable reports on security activity and compliance. The SIEM SecaaS service removes the enterprise tasks of log management, compliance reporting and security event monitoring. By moving these tasks and others to SecaaS, the enterprise eliminates the need for dedicated IT resources and their management.
- **Focus on core competencies—**SecaaS automates repetitive and resource-intensive security tasks, such as log management. Provisioning standard security services across business units or geographic regions can result in fewer common help desk calls and other IT management tasks, such as local procurement and server configuration. Eliminating these tasks frees enterprise resources to focus on core IT functions.
- **Scalability—** SecaaS offers rapid on-demand scalability. Enterprise information security infrastructure usage can be quickly scaled to meet new workload demands, whether up or down.
- **Fast provisioning—**SecaaS increases the speed of provisioning and de-provisioning users, devices and security applications. Enterprises can provision many users or security services on their own through the interface console or by calling the provider and requesting new services. These changes can be permanent or temporary, depending on the enterprise needs.
- **Best of breed—**SecaaS gives enterprises of all sizes affordable access to the most advanced information security services.
- **Expertise—**SecaaS gives the enterprise greater specialized security expertise than is typically available within an organization.
- **Continuous updates—**SecaaS provides continuous and automated security application and infrastructure updates that would require greater effort and resources if performed in-house.
- **Cost-effective compliance—**SecaaS can help an enterprise ensure that information security is in alignment with major compliance requirements, e.g., PCI DDS 2.0, Health Insurance Portability and Accountability Act(HIPAA), United Kingdom Data Protection Act, Statutory Audit and the Company Reporting Directives (EuroSox). Examples of SecaaS services that help the enterprise achieve compliance are:
  - SIEM, which reduces the enterprise cost of log management, compliance reporting and security event monitoring.
  - Tokenization of payment information, which removes customer payment data from the enterprise environment, achieves compliance with PCI DSS and maintains a high level of security. However, issues related to access to protected health information (PHI) must be evaluated to ensure that benefits and compliance are feasible.

---

[7] Blevins, Brandan; "Gartner forecasts rising interest in cloud-based security services," techtarget.com, 17 April 2013, *http://searchcloudsecurity.techtarget.com/news/2240181882/Gartner-forecasts-rising-interest-in-cloud-based-security-services*

[8] Gartner.com, "Gartner Says by 2015, 10 Percent of Overall IT Security Enterprise Product Capabilities Will Be Delivered in the Cloud," 15 April 2013, *www.gartner.com/newsroom/id/2426615*

[9] Rouse, Margaret; "Security as a Service (SaaS)," techtarget.com, August 2010, *http://searchsecurity.techtarget.com/definition/Security-as-a-Service*

[10] Microsoft.com, "Get Cloud Empowered. See How the Cloud Can Transform Your Business," *www.microsoft.com/global/el-gr/cloud/RenderingAssets/Hero/results/MyCloudPowerBrief_7607.pdf*

SecaaS Security and Risk Considerations

Even though SecaaS delivers security services, the enterprise remains accountable for security.

When exploring SecaaS as a security solution, an enterprise must consider several security factors. A SecaaS provider will likely offer some services, but it will not necessarily provide all of the services that the enterprise would provide if the security responsibility were completely in-house. It is imperative that the enterprise understand the gaps between what the enterprise expects and what the SecaaS provider will contractually provide when planning a comprehensive security solution. SecaaS covers many different security domains. The Cloud Security Alliance (CSA) released a set of documents that categorize SecaaS into 10 specific services:[11]

- **Identity and access management**
- **Data loss prevention**
- **Web security**
- **Email security**
- **Security assessments**
- **Intrusion management**
- **SIEM**
- **Encryption**
- **Business continuity and disaster recovery**
- **Network security**

The enterprise should answer the following questions, which span all of the SecaaS categories, before making the decision to deploy SecaaS:

- **What is the cloud service model that is best suited for our needs?**
- **Will the service process and/or store confidential information (network, vulnerability information, key material, etc.)?**
- **Where will the information be located and what retention policies will apply?**
- **How will data ownership be determined?**
- **How will the information be protected (physical and logical controls)?**
- **What are the contractual obligations, and how will they be enforced?**
- **What are the gaps between the service and a comprehensive security program?**
- **How will the gaps be addressed?**
- **How will we include the provider and outsourced services in the business continuity and disaster recovery plans?**
- **Can data be transferred to another provider if the contract is terminated?**

To answer these questions, the enterprise can consider the following topics.

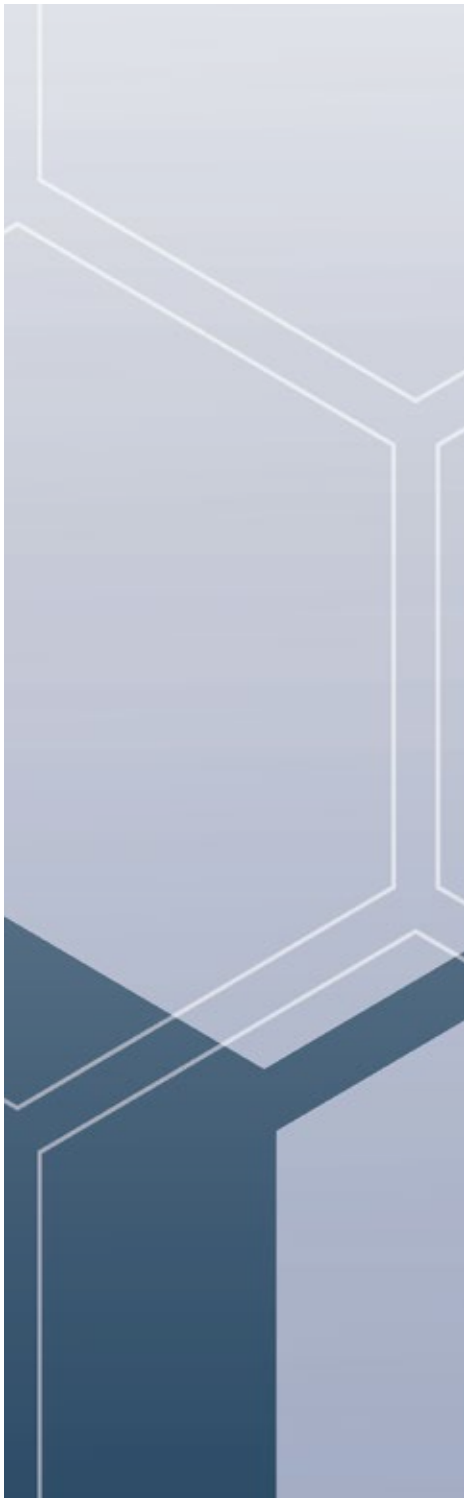
Service Model

A SecaaS service is usually deployed within a SaaS, PaaS or IaaS service model, depending on the layer that is being protected. Each offering requires different considerations. SaaS services push more layers of the infrastructure that typically would be on premise into the cloud. Most everything that SecaaS offers in a SaaS model is stored in a cloud service. In the PaaS model, the enterprise may have a bit more control around the offered platform and its configuration, but, most often, the SecaaS provider consumes and stores the confidential information that an attacker could easily exploit if exposed. In the IaaS model, the enterprise has even greater control over the layers running on the infrastructure; however, these services have visibility of the enterprise information while it is in transit.

Confidential Data

The enterprise is responsible for understanding the due diligence that is involved in ensuring that all critical information can be protected in alignment with internal policies and regulatory requirements. The first step for any enterprise should be to classify its data and understand whether any critical, confidential or private data will be processed and/or stored in a cloud environment. If the enterprise determines that data are to be stored in a less-than-optimal manner, the enterprise should seek to implement compensatory controls to reduce that risk.

[11] Cloud Security Alliance (CSA), "Introduction to Security as a Service," 21 March 2013, *https://cloudsecurityalliance.org/research/secaas/*



Data Protection

SecaaS providers are usually proficient at protecting critical and private data as part of their core activities. However, that does not mean that an enterprise should not research the solution set to ensure that it meets individual enterprise data protection standards. This research, or gap analysis, should be part of the due diligence that ensures that the service meets enterprise needs. Some things to consider when reviewing the offerings of the SecaaS provider are encryption algorithms, key management and user access provisioning. The enterprise should ask the following questions:

- **Are the provider's cryptographic key-storage procedures in line with the data protection requirements that the enterprise requires?**
- **Is access granted following the least privilege principle?**
- **Does the provider conduct access reviews according to the enterprise's policies?**
- **Are there any country-specific regulations that restrict the locations where data can be transferred, processed or stored?**

Contract

The enterprise should review the SecaaS contract with strict scrutiny, with a focus on understanding who is responsible for the specific security controls that the enterprise requires. Many contracts will push the ownership of data protection onto the enterprise via a service setting. The enterprise should ensure that the service security settings meet its needs, including regulatory compliance. The most important thing to remember during contract negotiations is that the enterprise is ultimately responsible for the security of its assets.

Gaps

When the contract and service review is complete, the contract usually will identify some instances where the SecaaS provider does not guarantee control compliance and the enterprise cannot comply because the system back-end services are not visible to the enterprise. These situations require a contractual agreement that includes some form of assurance that the enterprise can use to prove due care. In cases where the provider cannot allow back-end visibility, attestations, such as SSAE 16 (American Institute of CPAs [AICPA] Statements on Standards for Attestation Engagements) and ISAE 3402 (International Standards for Assurance Engagements), or certifications, such as ISO 27001 (International Organization for Standardization) or PCI DSS, can be requested by the enterprise as proof of adequate security. Small enterprises may not have the option to tailor the contract; therefore, any identified gaps must be managed as risk.

Strategies for Addressing SecaaS Risk

SecaaS deployment brings risk that may be beyond running and managing the security services in the enterprise in-house data center. Many enterprises may not have the expertise or the resources and staff that are required to effectively run and manage all security services. In these cases, SecaaS can be leveraged to complete the enterprise security solution. The risk of not having a complete suite of security services outweighs the risk of running SecaaS.

Understanding the differences and making sound management decisions is the key to successfully adopting SecaaS and securing an enterprise to the best level possible.

Commonly recognized risk management strategies are:

- **Acceptance—**Accept a risk, rather than mitigate, because avoidance or transfer costs are too high or not worth the investment.
- **Mitigation—**Establish physical, administrative and/or technical controls or systems that can help limit the scope and/or potential for problems that can result from risk. Risk should be mitigated to the level that is established as acceptable by the enterprise.
- **Avoidance—**Make changes to avoid the risk. Avoidance practices should be guided by the risk appetite defined by the enterprise.
- **Transfer—**Transfer the risk to another party (i.e., insurance). This is an avoidance strategy.

Risk management is a governance issue. The enterprise risk appetite designates its attitudes, its ability to control risk and its propensity to accept or avoid risk.

To be meaningful, IT risk measurement must originate and be addressed from consistent information security management systems (ISMSs) in an organized and systemic manner. Through the daily discipline of detecting, managing and reviewing operational IT risk, enterprises can create a risk baseline. With an established baseline, monitoring and exception reviews support root-cause analysis and systemic improvements that can improve the security posture of the enterprise. This approach is reflected in the ISO/IEC 27001:2005 standard Control Objectives and Controls. Similar concepts and the prevalent Plan/Do/Check/Act framework are pervasive in most mainstream risk management methodologies, including that of The Committee of Sponsoring Organizations of the Treadway Commission (COSO), and ISACA's COBIT 5 and Risk IT.

A central point to keep in mind in any analysis is that certain risk is the ultimate and nontransferable responsibility of every enterprise, whether it uses SecaaS or not.

The adoption of SecaaS (and other cloud services) is a significant architectural change that can introduce new risk and alter the effect of existing IT controls, simply because SecaaS displaces systems boundaries.

Significant differences exist between SecaaS setups and other IT architectures. To understand and assess how their information management controls may change with the introduction of SecaaS services into their infrastructure, enterprises must start from a known baseline of their systems. Because many SecaaS providers are not forthcoming in exposing their risk profile and factors, enterprises must verify the SecaaS provider risk/benefits equations.[12] A good rule to manage SecaaS providers is, "Trust, but verify."[13] The level of transparency that providers offer about their services and their internal security practices can vary. Transparency can be a good indicator of how much trust can be placed on the SecaaS provider and how much verification is needed to close any gaps and determine the real level of risk.

As a starting point, it is useful to examine how the boundaries of systems move in proposed SecaaS setups. Controls that used to exist within the safe and familiar boundaries of the enterprise's systems are now in the cloud environment.

[12] ISACA, "Calculating Cloud ROI: From the Customer Perspective," July 2012, *www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Calculating-Cloud-ROI-From-the-Customer-Perspective.aspx*
[13] Illustrated World of Proverbs, "Trust, but verify. Russian Proverb, American [19148]," 11 May 2012, *www.worldofproverbs.com/2012/05/trust-but-verify-russian-proverb.html*

Enterprises need to understand not only how they can attain their control objectives in the new environment, but also the control distortions introduced by the new systems topology.

The existing physical, administrative and technical controls of the enterprise must now be considered along with those of the SecaaS provider. If an enterprise wants to extend its controls into the physical space of the SecaaS provider, the enterprise needs to establish secure ways to access the SecaaS provider's systems. To obtain the cooperation of the provider and transfer information, new thinking and new systems design work may be required. To validate its control information, the provider may need to access the enterprise's systems, which requires that the enterprise set up secure information sharing protocols with the provider. In certain cases, special systems will need to be established within new, private, client/provider network boundaries. The technical infrastructure of the enterprise may have to be altered. All of these elements must be specified and assessed for risk impact, and control systems must be critically reviewed to determine what changes may need to be implemented in the new setup. The enterprise must conduct a gap analysis to evaluate the new architecture and determine whether the resulting set of controls is effective and meets the enterprise's needs in satisfactory ways.

Many executives and managers are eager to embrace cloud services because of their apparent ease of deployment, lower management burden, user friendliness and simplicity of use. These attributes, although they may even be real and demonstrable in some cases, can prove to be lures that result in costly consequences for service buyers. Users are prone to choosing convenience over security, which creates new and hard-to-control risk.

Cloud services can make it easy for users to circumvent IT controls and go around organizational boundaries. In most cases, data that have been moved to the cloud by a user can be accessed by that same user, or by someone else using his/her credentials, from outside the enterprise's network and downloaded or shared with unauthorized users, voluntarily or accidentally. Many users access confidential work documents over public WiFi infrastructure, for example, in airports or coffee shops. From a security perspective, such access defeats any security measures that may have been implemented by the enterprise to secure its own network, at whatever expense. Addressing this new situation (and other similar situations) requires a complete revision of the enterprise ISMS and, sometimes, the definition of new policies, procedures and controls.

Architecturally, cloud services resemble application service provider (ASP) services, with two major differences:

- **The border between the SecaaS provider and customer systems is changeable, which implies that it must be managed carefully.**
- **Because many Internet entities are looking for innocent victims, security must be actively managed at all times and with suitable expertise.**

Vendors have been known to make unsubstantiated promises about the security of their cloud offerings. Service buyers must independently test and verify vendor claims and assess whether vendor offerings meet the actual needs of their own organizations.

Enterprises have little control of data beyond the boundaries of their own systems, which can create new challenges. The way to address these challenges is to apply the same proven methodologies that enable an enterprise to secure its systems and data within its pre-SecaaS infrastructure.

In the cloud-based world, enterprises cannot grant trust on the basis of advertising or sales claims. Trust must only come as the result of a reasoned analysis that takes into account all the physical, administrative and technical parameters that can support consistent and effective risk management.

Governance

COBIT 5, from ISACA, provides a comprehensive framework that assists enterprises in achieving their objectives for the governance and management of enterprise IT.[14] Most relevant to this white paper is the first of the five key principles of COBIT 5—meeting stakeholder needs:

> *Enterprises exist to create value for their stakeholders. Consequently, any enterprise—commercial or not—will have value creation as a governance objective. Value creation means realising benefits at an optimal resource cost while optimising risk.*[15]

This principle also introduces the COBIT 5 goals cascade mechanism to translate stakeholder needs into specific, actionable and customized enterprise goals, IT-related goals and enabler goals.

Governance considerations for SecaaS should focus on making benefit, risk and resource assessment decisions by asking the following three questions:

- For whom are the benefits?
- Who bears the risk?
- What resources are required?

Benefits Realization Prerequisites

Before an enterprise can start to answer the three governance questions for its SecaaS solution, it must establish the following prerequisites.

The enterprise has an agreed on and common understanding of value from cloud computing in general.[16]
An enterprise can only achieve cloud computing benefits by articulating, understanding and agreeing on those benefits and effectively translating this understanding into the enterprise strategic goals and management plans.

SecaaS is just one of the cloud computing solutions that an enterprise might be exploring or implementing. Strategic direction

[14] ISACA, COBIT® 5, USA, 2012
[15] *Ibid.*
[16] More guidance is available from the white paper "Cloud Governance: Questions Boards of Directors Need to Ask," ISACA, April 2013, *www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Cloud-Governance-Questions-Boards-of-Directors-Need-to-Ask.aspx*

from the board and senior management for cloud computing assists the business, information security and IT teams with evaluating SecaaS benefits in the context of the enterprise goals. Not having a common understanding may result in *ad hoc* selection and implementation of a SecaaS solution, which, in turn, may result in wasted resources, accepting unwanted risk and suboptimal benefits realization for an enterprise.

The enterprise has a defined process to evaluate and monitor benefits realization.
Most enterprises require a business case or equivalent processes to get funding or spending approvals. A defined process to articulate potential benefits helps stakeholders by facilitating senior management's evaluation of the SecaaS benefits, and helps the assurance function during their assessment and verification of benefits realized against those planned.

Additional guidance from service providers and publications, such as *"Calculating Cloud ROI: From the Customer Perspective,"*[17] might help to facilitate the preparation of the business case for a SecaaS solution.

The enterprise has assigned an owner for its SecaaS solution.
Establishing accountability up front is crucial for any successful project or process. SecaaS solution accountability can be assigned to the business or IT process owner, depending on its business requirements context. Although accountability of a SecaaS solution may be assigned to the business team or function that is realizing the most benefit from it, responsibility for acquisition, deployment and operations for the SecaaS solution can be understood to be with the information security or IT team.

Risk Optimization Prerequisites

The enterprise has an agreed on and common understanding of cloud computing risk based on an enterprise risk management (ERM) framework.
Value and risk are considered as two sides of the same coin. Similar to the importance of understanding value from cloud computing, it is equally important to articulate, understand and agree on risk and security considerations for cloud computing. Risk threshold levels in selecting and implementing a SecaaS solution should be evaluated and approved against enterprise acceptable risk and tolerance levels.

In the absence of an ERM framework, cloud computing risk and a SecaaS solution should be considered at the executive level. Additional guidance is available from the following ISACA publications:

- **Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives**[18]
- **Security Considerations for Cloud Computing**[19] (includes guidance on security risk and threats related to operating in the cloud and the path to the decision)

The enterprise has defined processes and controls to support quick response to changing risk and immediate reporting to appropriate levels of management.
Once a decision is made to implement a cloud computing solution including a SecaaS, the business and IT teams should identify the processes and controls to manage solution risk, related IT risk and enterprise risk, to an acceptable level. The processes and controls should be defined and communicated at appropriate levels to support quick response to changing risk and immediate reporting to appropriate levels of management. This support ensures that appropriate incident and risk response actions are taken to bring back and maintain the acceptable level of risk. Root cause analysis during incident response and as part of postincident review can be considered to ensure that appropriate management corrective actions are taken.

The enterprise seeks assurance periodically to ensure solution effectiveness and to maintain stakeholder transparency.
The enterprise should determine assurance objectives for its cloud computing strategy and environment based on assessment of the internal and external environment/context and of the relevant risk and related opportunities. A combination of self-assessment, internal audit/assessment and external audit/assessment can be considered by an enterprise taking into account the risk exposure and complexity of a SecaaS solution.

[17] ISACA, "Calculating Cloud ROI: From the Customer Perspective," July 2012, *www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Calculating-Cloud-ROI-From-the-Customer-Perspective.aspx*

[18] ISACA, "Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives," September 2010, *www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Cloud-Computing-Business-Benefits-With-Security-Governance-and-Assurance-Perspective.aspx*

[19] ISACA "Security Considerations for Cloud Computing," September 2012, *www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Security-Considerations-for-Cloud-Computing.aspx*

The enterprise should consider assurance requirements while defining Service Level Agreements (SLAs) with SecaaS providers and, if possible, including the requirements in the contract to establish vendor accountability.

Mechanisms for ensuring the accuracy and reliability of mandatory reporting should be established and assessed periodically to maintain stakeholder transparency.

Resource Optimization Prerequisites

The enterprise has identified and documented the resources required.

Business requirements identified at earlier governance stages should now be translated into functional and technical requirements. The information security and IT teams can benefit from research documents that are available from organizations, such as the CSA, to guide their efforts before, during and after a SecaaS implementation. The CSA documents[20] about SecaaS focus on categorizing different types of SecaaS products and provide guidance on reasonable implementation practices.

The enterprise should consider an internal and external resource mix to optimize cost/benefits from a SecaaS solution. The enterprise should also consider defining processes and procedures to support and integrate a SecaaS solution within the enterprise and to determine how resources should be allocated to each process.

Roles and responsibilities for solution acquisition, deployment and operations are defined and communicated.

The enterprise should not only consider internal roles and responsibilities but also external parties. These external parties may include the SecaaS provider, system integrators, third-party contractors and external auditors. The entire life cycle of any SecaaS solution, i.e., from requirements definition to solution acquisition, deployment, operations and improvement, until retirement, should be considered when defining roles and responsibilities.

From an external perspective, roles and responsibilities can be defined in an SLA or contract. From an internal perspective, roles and responsibilities can be defined in an Operational Level Agreement (OLA) or process/procedure documentation. This documentation should be reviewed by the parties involved and updated as required. The locations of these documents should be communicated and made available to all internal and external resources, when and where needed.

The enterprise has defined measures to assess performance and support informed decision making.

Without defined performance measure processes, management at any level will find it difficult to make informed decisions.

The enterprise performance measure processes should include both quantitative (where possible) and qualitative measures and metrics to evaluate, direct and monitor resource management.

During the solution evaluation stage, an enterprise should review and, where possible, influence the SecaaS SLA that will facilitate performance measurement from an external perspective. The measures and metrics should be agreed on by internal parties to ensure that responsibilities are well understood and resources are allocated and utilized as planned.

When Enterprises Do Not Meet the Prerequisites

Most enterprises will not meet all of the prerequisites Alternatively, if an enterprise implemented a SecaaS solution in an *ad hoc* manner, these prerequisites may remain unmet. When governance and management concepts are ambiguous or not clear at the executive level and/or at the IT function level, meeting the prerequisites can be a challenge. The information security or IT team should articulate and communicate these prerequisites, and, where possible, document them.

The audit/assurance team can also benefit from using the prerequisites to assess a SecaaS solution's governance effectiveness. This team may be the change agent that triggers a discussion among business and IT teams to consider defining governance and management practices for enterprise IT.

[20] More details are available at *https://cloudsecurityalliance.org/research/secaas/*.

Assurance Considerations for SecaaS

Enterprises implement controls of various types (technical, administrative, physical, etc.) to protect the Confidentiality, Integrity, Availability and Authenticity (CIAA) of their information. When the controls are in place, the enterprise needs assurance that they are working as intended. However, assurance in the cloud may be more difficult to achieve than for systems onsite due to the reduced visibility into the provider's environment and practices. Assurance for SecaaS may be better accomplished by establishing a partnership with the service provider to implement monitoring and reporting mechanisms (internal and third-party) that allow the enterprise to assess periodically the adequacy and effectiveness of controls against the changing threat landscape.

The first step in establishing an assurance program for SecaaS is to understand each party's role.

The enterprise may lose control over processes and data, but it retains full accountability for security and compliance.

The SecaaS provider is only responsible for the operational portion of the equation.

Assurance considerations for SecaaS are very similar to those needed for any other cloud-based service; however, for SecaaS, the focus should be on availability, privacy, data security, location and compliance, as follows:

- **Availability—**Most information security services are required to function 24/7 to provide continuous protection of data at rest and security services are required to function 24/7 to provide continuous protection of data at rest and during processing and transfer. SecaaS providers must be able to demonstrate the existence and efficient performance of controls that ensure availability of security services, as determined by the SLA.
- **Privacy—**Providing services such as identity access management and email security may require SecaaS providers to have access to private data; therefore, the provider should demonstrate that its security environment has effective controls that protect the privacy of any personally identifiable data and communications from any unauthorized disclosure. Controls to detect and respond to breaches are also important and must be included in any assurance evidence provided by SecaaS providers.
- **Data security—**Enterprises using SIEM services need assurance that logs are protected against unauthorized disclosure, destruction and corruption. SecaaS providers must assure that controls are in place to protect data confidentiality, integrity and availability and that those controls are tested periodically to confirm effectiveness.
- **Location—**The physical location of SecaaS providers (including third-party providers) dictates the jurisdiction and legal obligations that the enterprise must obey. Countries have different laws protecting personally identifiable information and compliance requirements. The rights that governments have to request data from service providers when conducting investigations are also considerably different among countries. SecaaS providers must disclose the locations that will be involved in providing services for a particular enterprise so that the enterprise can determine whether those locations represent an issue. Providers must also disclose when a merger or acquisition is being considered, to allow the enterprise to assess whether new geographic locations will represent a jurisdictional, compliance or legal risk.
- **Compliance—**Enterprises using SecaaS as a means to comply with regulations need to be aware of any changes that may impact (break) their compliance posture. SecaaS providers must allow visibility into the change management process to enable enterprises to assess the impact of upcoming changes.

The decision to establish a partnership with a SecaaS provider may depend on the level of visibility and disclosure that the provider is willing to grant. Visibility and disclosure should be discussed during the negotiation phase and should be part of the selection criteria.

"Trust, but verify." [21] Because security and compliance accountability cannot be transferred when contracting SecaaS providers, enterprises should implement internal controls to manage expectations and provide management with the necessary assurance to trust the SecaaS providers. Some controls that can be used to accomplish this follow.

Monitoring Controls

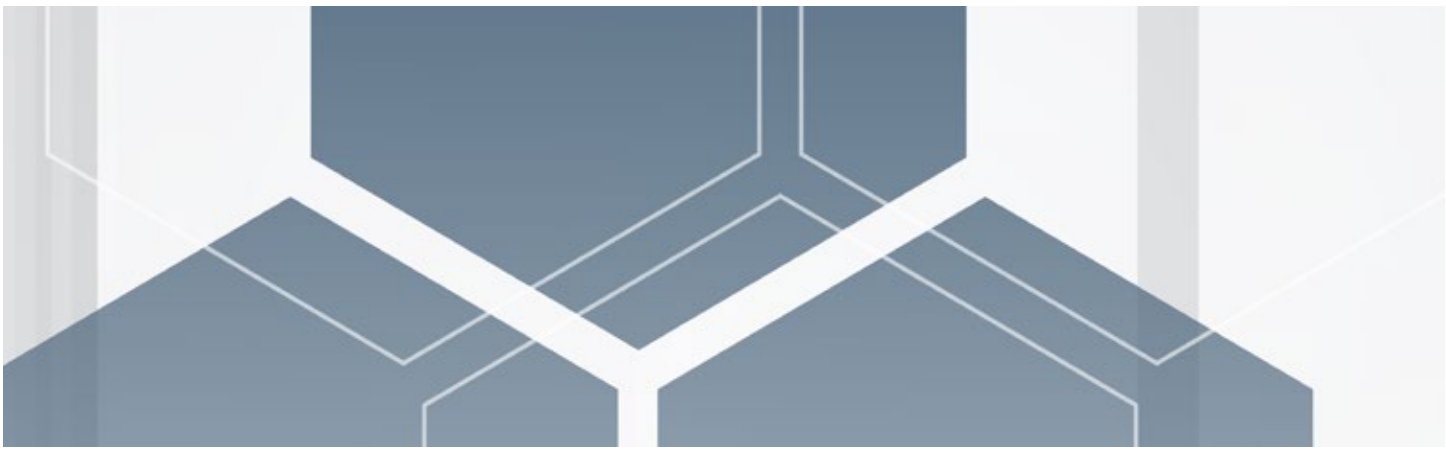
Enterprises should use SLAs to monitor and assess the performance and conformance of SecaaS providers. Performance and compliance must be reviewed continuously and consistently by business process owners, IT, vendor management and risk management to identify any gaps that must be addressed to ensure that all requirements are met as expected.

Reporting Controls

To compensate for the inability to audit the environment of providers, enterprises must request proof that the security environments meet applicable policies, business needs and regulatory and legal requirements. Usually, this proof is in the form of independent security reviews or certification reports issued by third parties to attest that the security environment meets a particular set of standards. Some of the most common standards used to assess the adequacy of a provider's security environment are: Cloud Security Alliance Trust and Assurance Registry (STAR), ISO, PCI DSS, HIPAA, US Sarbanes-Oxley Act of 2002 and EuroSOX, Federal Information Processing Standard (FIPS) 140-2, and AICPA SSAE Service Organization Controls (SOC) 2 reports (can be used by SecaaS providers as proof of independent review), in addition to any other regulatory certification required. In the UK, ISAE 3402 reports serve the same purpose. The type of certification or report varies across countries and industries, but the importance and relevance are the same.

Compensatory Controls

The enterprise must implement controls to address any gaps that are identified during the SecaaS-provider selection and contract negotiation phases. Compensatory controls should also be implemented to manage new risk that is introduced by changes to the IT environment to integrate SecaaS. These compensatory controls can include governance (e.g., new policies and procedures, user training, frequent risk assessments and training on SLA management), physical (e.g., network segmentation and traffic filters) and logical controls (e.g., restrict privilege accounts, encryption and federated identity management).



[21] Illustrated World of Proverbs, "Trust, but verify. Russian Proverb, American [19148]," 11 May 2012, *www.worldofproverbs.com/2012/05/trust-but-verify-russian-proverb.html*

Conclusion

Never before has there been such rapid expansion in both the depth and breadth of demand for security services. Traditional methods of delivering information security—small teams of specialists operating within IT functions—are straining to keep up with the fast-paced and constantly evolving threats to enterprise information assets. SecaaS promises to deliver the scope, scale and sophistication of tools required to protect enterprise information, while substantially decreasing the costs and resources associated with information security. The benefits of using SecaaS come with risk that enterprises must be willing to address to make SecaaS a valuable solution. Using a third party to provide critical services requires an enterprise to relinquish some control, but the enterprise is always accountable for information security assurance, no matter where the information resides or which party controls it.

By using the comprehensive COBIT 5 framework for the governance and management of enterprise IT, enterprises can determine the functions that realize the SecaaS benefits and bear the risk and the resources required to implement a SecaaS solution. The framework provides an assurance model to test the controls that protect the enterprise information assets.

The level of responsibility for controls and assurance varies across the SecaaS provider and the enterprise. The enterprise should create a partnership with the SecaaS provider and encourage transparency of security controls and open communication. Working with the SecaaS provider to build an SLA that protects the enterprise's information assets and processes ensures that the enterprise has visibility and control over all assets, whether on- or off-site, and that the enterprise can realize sustainable value from SecaaS.