Presented to the Interdisciplinary Studies Program:

UNIVERSITY OF OREGON
APPLIED INFORMATION MANAGEMENT

Applied Information Management
and the Graduate School of the
University of Oregon
in partial fulfillment of the
requirement for the degree of
Master of Science

How Cloud Computing (SaaS) Supports an Electronic Document and Records Management System (EDRMS)

CAPSTONE REPORT

John R. Hidalgo
Information Manager
Macquarie Infrastructure & Real Assets Inc.

University of Oregon
Applied Information
Management
Program

July 2013

Continuing Education
1277 University of Oregon
Eugene, OR 97403-1277
(800) 824-2714

Approved by

Dr. Linda F. Ettinger
Senior Academic Director, AIM Program

How Cloud Computing (SaaS) Supports an Electronic Document and Records Management System (EDRMS)

John Hidalgo

Macquarie Infrastructure & Real Assets Inc.

Abstract

This annotated bibliography identifies literature published from 2007 to 2013 that examines the use of cloud computing (specifically software-as-a-service [SaaS] in support of an electronic document and records management system (EDRMS). The goal is to examine two factors: (a) cost effectiveness and (b) information security. Findings show that cost is affected by the type of cloud deployment model and particular use. A key security issue is regulation, which can be mitigated through audit and monitoring.

Keywords: cloud computing, SaaS, edrms, records management, RIM, information security

Table of Contents

Introduction to the Annotated Bibliography

Problem Area

Information records have value in an organization and add to the worth of the organization (ARMA International, n.d.) (a). Every organization, including federal agencies, must address objectives that will add value by achieving the organizations goals or by reducing cost (NARA). In order to realize this value, today's businesses need to be flexible in ways to access information because there is constant change in many directions, for example through mergers, acquisitions, new regulations, competition, economic pressures (Hai, Sakoda, & Fujitsu 2009). Businesses are also faced with constant technological change, aging infrastructure and software, shrinking budgets, and a global and mobile workforce (Farrell, 2010). To keep the informational value, companies continue to invest in IT infrastructure rather than have issues such as, i.e. outdated and no longer supported software, expensive to maintain hardware, lack of agility, and other problems that can make IT a hindrance (Symons, 2008). As a result, one of the questions facing businesses today is whether to house organizational information (e.g. records) on premise or off, e.g., in the cloud (Bibi, Katsaros & Bozanis, 2012).

Records management systems enable records to be managed from creation to destruction (EDRMS, 2013). These systems are referred to as electronic document and records management systems (EDRMS, 2013). EDRMS is a type of content management system that combines the technologies of document management and records management systems as an integrated system (EDRMS, 2013).

According to Mell and Grance (2011), the National Institute of Standards and Technology (NIST) defines cloud computing "as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort of cloud provider interaction" (p.2). Cloud computing claims to address these concerns (and more) by leveraging on-demand reliable computing services from an external provider (Jansen & Grance, 2011).

Jansen & Grance, 2011 describe three well known service models for cloud computing: (a) software-as-a-service; (b) platform-as-a-service; and (c) infrastructure-as-a-service.

- Software-as-a-service (SaaS) is a model of service delivery of one or more applications along with the computing resources to run them are provided for use on demand. SaaS's main purpose is to reduce the total cost of hardware and software development, maintenance and operations.
- Platform-as-a-service (PaaS) is a model of service delivery where the computing platform is provided on demand in which applications can be developed and deployed. PaaS's main purpose is to reduce the cost and complexity of purchasing, storing, and managing hardware and software components of the platform.
- Infrastructure-as-a-service (IaaS) is a model of service delivery where the basic computing infrastructure is provided. This infrastructure includes servers, software, and network equipment. Its main purpose is to avoid purchasing, storing, and managing the hardware and software infrastructure components. These components are managed through a service interface and the consumer has broad freedom to choose their own operating system.

One component of cloud computing that is becoming popular among organizations is *software as a service* (SaaS) (McAffee, 2012). SaaS is a software delivery model in which software and data are centrally hosted on the cloud and which is typically accessed by users using a web browser (Software as a service, 2013). SaaS provides network-based access to commercial software and, according to Orlando (2011), represents the potential for a low-cost strategy for businesses to using software on demand rather than buying a license for every computer. According to Bibi (2012), there are three factors pushing the adoption of SaaS-based solutions and the cloud in general: (a) potential cost reductions; (b) reduce implementation complexities; (c) and pressure to innovate.

Purpose

An EDRMS is an electronic document and records management system designed to facilitate the creation, management, use, storage, and disposal of both physical and electronic records (State Records NSW, n.d.). Electronic records management (ERM) is the field of management responsible for the systematic control, creation, receipt, maintenance, use and disposition of records (AIIM, 2013c). As noted by Ferguson-Boucher and Convery (2011), electronic records management systems are available today in the cloud. The purpose of this annotated bibliography is to identify and present literature that examines the use of cloud computing (specifically software-as-a-service [SaaS]) (Hai, Sakoda, & FUJITSU, 2009) in support of an electronic document and records management system (EDRMS).

The goal in this study is to examine two factors related to use of the SaaS option in this context: (a) cost effectiveness (Bibi, Katsaros & Bozanis, 2012), and (b) information security (Kamal & Kaur, 2011). Selected literature concerning cost and information security is analyzed in relation to strengths, weaknesses, opportunities, and threats (i.e., the SWOT analysis evaluation framework) (Humphrey, 2005). Using SWOT provides a way to examine SaaS and identify what it does well in relation to *cost* and *information security* and what may need improvement (SWOT analysis, 2013).

Research Questions

The main research question addressed in this study is: How does the software as a service [SaaS] model support an electronic document and records management system (EDRMS) in relation to cost and information security? Four sub-questions guide this study: (a) what is the current definition of SaaS; (b) what is the current definition of an EDRMS; (c) what are the strengths, weaknesses, opportunities, and threats concerning *cost*, related to use of SaaS in support of an EDRMS; and (d) what are the strengths, weaknesses, opportunities, and threats concerning information *security*, related to use of SaaS in support of an EDRMS?

Audience

The annotated bibliography is intended for information management and records management professionals who are responsible for researching and implementing cloud computing, specifically SaaS, to be used with an EDRMS. The definition of a records management professional according to expertglossary.com:

> The records manager is responsible for the implementation of a records management program in keeping with the policies and procedures that govern that program, including the identification, classification, handling and disposition of the organizations records throughout their retention life. The physical storage and protection of records may be a component of this individual’s functions, but it may be delegated to someone else. (Records Manager, n.d.)

The definition of information management according to Association for Information and Image Management (AIIM):

> Information management (IM) is the collection and management of information from one or more sources and the distribution of that information to one or more audiences. This

> sometimes involves those who have a stake in, or a right to that information.
>
> Management means the organization of and control over the structure, processing and delivery of information. (AIIM, 2013b)

According to Empel (2012), information management professionals should decide how records are created and captured and which technologies will support these processes. As businesses consider new opportunities for information management initiatives in reducing costs and eliminating legacy systems and data, "records managers will have the opportunity to shape policy, alongside their colleagues in the IT and legal departments" (Shute, 2012, p.23).

Significance

The use of cloud computing services is becoming more widespread in both public and private organizations (Ferguson-Boucher & Convery, 2011). Cloud computing services are purported to leverage local business computing services by using large data centers that enable a reduction of the cost of using information technology through efficient resource utilization (Ferguson-Boucher & Convery, 2011). Organizations are promised that they can access the cloud services in a cost efficient manner via an internet connection on demand and on a subscription basis without having to invest in their own IT infrastructure (Ferguson-Boucher & Convery, 2011).

According to Berg (2011), cloud computing is being regarded as the answer to modern record keeping. Cloud computing means shrinking the need for managing vast amounts of data on expensive, aging, energy-inefficient, on premise servers (Berg, 2011). Another strength noted by Berg (2011) is scalability in which a service is offered as pay as you go in purchasing server space, which can handle spikes in usage (Berg, 2011). For example, the State of Oregon is working with Autonomy, an HP company, on a cloud-based records management system that will allow state, city and county agencies to manage, secure, and provide access to digital documents (Shum, 2013). The White House and the Office of Management and Budget (OMB) are encouraging government agencies to reap the promised benefits of cloud computing and many federal offices have already begun the transition (Berg, 2011).

According to Barnes (2010), records and information management (RIM) professionals cannot afford to be out of touch with cloud computing for data storage and retrieval. As the transition to a RIM cloud environment continues to evolve and the technology is increasingly complex, records managers need to understand the opportunity (Barnes, 2010).

Delimitations

Time frame. The references provided in this study are published between 2007 and 2013. The period covers the most up to date information on cloud computing usage in relation to SaaS and EDRMS. The time frame excludes older research before 2007 to ensure the information in this annotated bibliography is relevant to current challenges.

Audience. This annotated bibliography is targeted to Records and Information Management professionals who work in organizations that require their input on cloud computing solutions using SaaS for EDRMS. Businesses are transitioning to a RIM cloud environment and the technology is increasing complex (Barnes, 2010). Companies can include the RIM professionals when deciding to use cloud solutions.

Topic focus. The transition to a cloud-based records and information management environment continues to evolve with the help of SaaS and EDRMS (Barnes, 2010). The literature selected for use in this annotated bibliography is framed by the perspective presented by Ferguson-Boucher and Convery (2011) who say that SaaS is an area of "interest to the record and information management community for the future but adoption is dependent on evidence of the security of the cloud providers' services and infrastructure" (p. 8).

Analysis approach. The strengths, weaknesses, opportunities, and threats (SWOT) analysis method is selected as a way to analyze SaaS as support for an electronic data and records management system, in relation to cost and security. The choice to use the SWOT approach is based on this researcher's belief that it is best to attempt to get past the marketing hype behind the notion of the positive value of SaaS and instead find an analytic method that supports a more balanced assessment. SWOT can identify the key internal and external factors seen as important to achieve an objective (SWOT analysis, 2013).

Reading Plan Preview

The reading plan for this Annotated Bibliography utilizes conceptual analysis (Busch, De Maret, Flynn, Kellum, Le, Meyers, Saunders, White, & Palmquist, 2012) that provides a process to examine the selected references in relation to key concepts embedded in the research questions. This approach is designed to verify the presence of certain words and/or concepts through a process known as coding (Busch et al., 2012). According to Busch et al. (2012) the steps in the conceptual analysis coding process are:

1. Decide the level of analysis.
2. Decide how many concepts to code for.
3. Decide whether to code for existence or frequency of a concept.
4. Decide on how you will distinguish among concepts.
5. Develop rules for coding your texts.
6. Decide what to do with irrelevant information.
7. Code the texts.

Organizational Plan Preview

The categorization of the selected references located in the Annotated Bibliography section of this paper is organized around a set of themes (Literature Reviews, n.d.). In this Annotated Bibliography, four main themes are explored in detail: (a) current definitions of SaaS, (b) current definitions of EDRMS, (c) SWOT analysis related to security when using SaaS in support of an EDRMS, and (d) SWOT analysis related to cost when using SaaS in support of an EDRMS. This same organizational plan is used to provide the audience with a clear discussion of the coding process results, which are presented in the Conclusions.

Definitions

The following definitions are listed in order to provide readers with the understanding of the terminology used in this annotated bibliography. The definitions below have specific meaning to SaaS and EDRMS, as these terms are used in this study. The terms *EDRMS*, *electronic document records management systems*, and *records management systems* are used synonymously.

AIIM (Association for Information and Image Management) – The global community of information professionals. We provide the education, research and certification that information professionals need to manage and share information assets in an era of mobile, social, cloud and big data (AIIM, 2013a).

Application programming interface (API) – Specifies how some software components should interact with each other. In practice in most of the cases an API is a library that usually includes specification for routines, data structures, object classes and variables (Application programming interface (n.d.).

ARMA International – A not-for-profit professional association and the authority on managing records and information – paper and electronic (ARMA International, 2013b).

Cloud computing – Cloud computing is a model for enabling ubiquitous convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models" (Mell & Grance, 2011).

Cloud providers – A service provider that offers customers storage or software services available via a private (private cloud) or public network (cloud). The storage and software is available for access via internet (Cloud Provider, n.d.).

EDRMS (electronic document and records management system) – Is a type of content management system and refers to the combined technologies of document management and records management systems as an integrated system (EDRMS, 2013).

IEEE (Institute of Electrical and Electronics Engineers) Computer Society – The IEEE Computer Society is the computing professional's single, unmatched source for technology information, inspiration and collaboration. By making the most up-to-date and advanced information in the computing world easily accessible, we are the source that computing professionals trust to provide high quality, state-of-the-art information on an on-demand basis.

Information Security – The protection of information and the systems and hardware that use, store, and transmit that information (Whitman & Mattord, 2010).

Multitenancy - Refers to a principle in software architecture where a single instance of the software runs on a server, serving multiple client organizations (tenants). With a multitenant architecture, a software application is designed to virtually partition its data and configuration, and each client organization works with a customized virtual application instance (Multitenancy, 2013).

NARA – The National Archives and Records Administration (NARA) is the nation's record keeper. Of all documents and materials created in the course of business conducted by the United States Federal government, only 1%-3% are so important for legal or historical reasons that they are kept by us forever (NARA, n.d.).

NIST (National Institute of Standards and Technology) – Founded in 1901, NIST is a non-regulatory federal agency within the U.S. Department of Commerce. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life (US Department of Commerce, n.d.).

Record – Recorded information, regardless of medium or characteristics, made or received by an organization in the pursuance of legal obligations or in the transaction of business (ARMA International, 2013a).

Records Manager – The records manager is responsible for the implementation of a records management program in keeping with the policies and procedures that govern that program, including the identification, classification, handling and disposition of the organizations records throughout their retention life. The physical storage and protection of records may be a component of this individual's functions, but it may also be delegated to someone else (Records Manager, n.d.).

RIM – Records and information management (RIM) is the field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use, and disposition of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records. Records, therefore, have value and add to the intrinsic worth of the organization. Records need to be managed in a meaningful way so they can be accessed and used in the course of daily business functions throughout the organizational environment (ARMA International, 2013c).

SaaS (Software as a Service) – Software that is owned delivered and managed remotely by one or more providers. The provider delivers software based on one set of common code and data definitions that is consumed in a one-to-many model by all contracted customers at any time on a pay-for-use basis or as a subscription based on use metrics (Gartner, n.d.).

Society of American Archivists - Founded in 1936, the Society of American Archivists is North America's oldest and largest national archival professional association. SAA's mission is to serve the educational and informational needs of more than 6,000 individual and institutional members and to provide leadership to ensure the identification, preservation, and use of records of historical value (Society of American Archivists, n.d.).

SWOT – Is a structured planning method used to evaluate the strengths, weaknesses, opportunities, and threats involved in a project or in a business venture (SWOT analysis, 2013).

Virtualization – In computing, virtualization is simulating a hardware platform, operating system, storage device, or network resources (Virtualization, n.d.).

Research Parameters

This section of the document defines the research design of this annotated bibliography. It describes the search process, keywords, databases used, evaluation criteria for literature selection, and processes to document (a) the references and (b) information identified during data analysis.

Search Strategy

This study is limited to selected literature addressing SaaS and electronic document and records management systems (EDRMS) that provide information and discussion on cost and information security measures. It does not include an exhaustive list of SaaS providers that support EDRMS.

The initial search strategy consisted of using the University of Oregon's libraries and databases against the following key search terms: *information governance, cloud computing, cloud information security,* and *SaaS*. Terms are refined to include *electronic document and records management system* (EDRMS), *SaaS and records management, SaaS and EDRMS,* and *information security*.

Using the UO Libraries, the following peer-reviewed journals are located through the database Academic Search Premier: (a) *News Media & the Law,* (b) *Information Management Journal,* and (c) *IEEE Security Privacy*. Using Google scholar, the following sources are located: (a) *Journal of the Society of Archivists,* (b) *NIST special publication,* (c) *Reuters,* and (d) *Asia Pacific Journal of Information Systems*.

Selected literature is retrieved via the University of Oregon online libraries and databases, Google Scholar, professional publications, journals, and personal collections. The selection of literature is limited to authors who are members of, or affiliated with:

- Professional organizations: including ARMA International, AIIM, IEEE Computer Society, Society of American Archivists, National Institute of Standards and Technology (NIST).
- U.S. and foreign government agencies.
- Selected academic institutions including University of Oregon, and Colorado State University.

Documentation Approach

The method to document research material is done through computer software called Zotero. Zotero is a powerful research tool that assists in gathering, organizing, and analyzing sources such as citations, full texts, web pages, images, and other objects (Zotero, n.d.). Zotero is installed in the Firefox web browser which is used to conduct all searches. Once relevant and useful literature is found, content and references are saved using Zotero's built in browser utility and organized into my library collection within Zotero. The collection library within the Zotero libraries represents this annotated bibliography. The library collection is organized into the following categories:

- Cloud security
- Complications of cloud
- Definitions
- EDRMS definition
- Information / records management
- Information security
- Records & cloud
- Reference credentials

- SaaS & records management
- SaaS & cost
- SaaS definition
- SaaS Security
- SWOT analysis

Evaluation Criteria

To ensure the credibility and relevance of materials to this research, the materials must show relevance and credibility (Bell & Frantz, 2012). Specific evaluation criteria include:

Authority. Author's credentials are examined by examining professional affiliations to known organizations and other writings by the author. The publisher credentials are also examined to find their specialization in the field. Both author and publisher reputations are examined by conducting web searches to search other works and reputation.

Objectivity. The literature is reviewed for a point of view, bias acknowledgement, and cited evidence to support arguments and conclusions.

Quality. The quality of the literature is reviewed for (a) well organized and structured information, (b) main points clearly presented, (c) good grammar, (d) spelling mistakes or typographical errors, and (e) cited credible sources.

Currency. The date of the publication is considered. This study is limited to published literature between 2007 and 2013.

Relevancy. The relevance of content is reviewed whether the literature is appropriate for the research question and sub questions. Further review is needed to establish content that is scholarly or popular.

Reading Plan

The reading plan follows a process known as conceptual analysis (Busch et al., 2012). This analysis process provides a way to examine the selected references in relation to key concepts embedded in the research questions. This approach is designed to verify the presence of certain words and/or concepts through a process known as coding (Busch et al., 2012). Once the selected references have met the evaluation criteria noted above, the process of coding is conducted using the following seven steps:

Level of analysis. The words and phrases that define the level of analysis in this annotated bibliography include cloud *computing, SaaS, electronic document and records management system* (EDRMS), and *information security*. Other phrases that define the level of analysis include *cloud information security* and *SaaS records management*.

Quantity of concepts. There are four pre-defined areas for consideration in this annotated bibliography: (a) current definition of SaaS; (b) current definition of an EDRMS; (c) the strengths, weaknesses, opportunities, and threats concerning *cost,* related to use of SaaS in support of an EDRMS; and (d) the strengths, weaknesses, opportunities, and threats concerning information *security,* related to use of SaaS in support of an EDRMS. Key terms and phrases are added in an emergent fashion, if they are identified as relevant and appropriate.

Code for existence or frequency. This study is coded for existence of words or phrases in order to determine the meaning. The number of times a word or reference appears in a reference is not in scope.

Distinguish concepts. Concepts that are similar in meaning are coded as one. For example, *software as a service* is coded as one with *SaaS*. Other terms that are coded together include *electronic document records management system* and *EDRMS, cloud computing* and *cloud,* and *information security* with *security.*

Rules for coding. Coding exists for key concepts, as well as sub-concepts. For example, coding for *EDRMS* includes coding for the related sub-concepts of *electronic documents, records management system,* and *records.*

Irrelevant information. For this annotated bibliography, unrelated content is excluded.

Code the texts. References identified are coded through a combination of computer based and manual coding procedures. Concepts are first run through a computer search to look for key words and phrases. Additional coding is done manually to ensure similar meanings are not missed by an automated process.

Organizational Plan

The key references presented in the Annotated Bibliography section of this paper are organized thematically (Literature Reviews, n.d.) according to the themes derived from the main research questions and sub questions. The four themes used in the organization are: (a) current definitions of SaaS, (b) current definitions of EDRMS, (c) SWOT analysis related to security when using SaaS in support of an EDRMS, and (d) SWOT analysis related to cost when using SaaS in support of an EDRMS.

The first theme of the definition of SaaS cloud computing defines the term in accordance to current industry and professional organization definitions (Healey, 2010) (Mell & Grance, 2011).

The second theme of the definition of EDRMS defines the term in accordance to current industry and professional organization definition and applied concepts (State Records NSW, n.d.) (Empel, 2012).

The third theme is a SWOT analysis focusing on SaaS security in support of an EDRMS. This theme presents resources that explore security environments in using SaaS as a cloud records management service (Benlian, 2011) (Veiga & Eloff, 2010).

The fourth theme is a SWOT analysis focusing on cost in support of an EDRMS. This theme presents resources that explore costs in implementing SaaS as a records management service (Bibi, Katsaros, & Bozanis, 2012) (Foley, 2012).

References which highlight only specific topics are categorized under that theme. Other references, which highlight multiple topics, are aligned with the closest relevant theme.

Annotated Bibliography

The main research question addressed in this study is: How does cloud computing (software as a service [SaaS] support an electronic document and records management system (EDRMS) in relation to cost and information security? Four sub-questions guide this study: (a) what is the current definition of SaaS; (b) what is the current definition of an EDRMS; (c) what are the strengths, weaknesses, opportunities, and threats concerning *cost*, related to use of SaaS in support of an EDRMS; and (d) what are the strengths, weaknesses, opportunities, and threats concerning *information security*, related to use of SaaS in support of an EDRMS?

Key references are presented below, organized in relation to each of the research sub-question topics. Annotations consist of four elements: (a) the bibliographic citation in APA format; (b) the published abstract; (c) a description of the credibility of the reference; and (d) a summary of the relevant content, related to the research questions addressed in this study.

The following set of references provides current definitions of SaaS cloud computing.

Barnes, F. R. (2010). Putting a lock on cloud-based information. *Information Management Journal*, *44*(4), 26–30.

Abstract. The article offers information on the significance of cloud technology to companies in the U.S. It mentions that the said technology data can be transferred, transmitted and stored in any virtual environment at an affordable cost. It states that cloud technology also enables transmission of data through the Internet via high speed broadband communications system. To keep abreast with the latest developments in cloud technology, it suggests that records information management (RIM) professionals should keep in touch with the latest trends in cloud.

Credibility. Frederick Barnes is a graduate of Brown University and holds a juris doctor degree from the University of Kansas. Fredrick is a published author for the Information Management Journal – an ARMA International publication.

Summary. Barnes introduces a primer on cloud computing and describes the collaboration that is needed between RIM and IT professionals for the use of cloud computing in organizations. Barnes introduces a "layered approach" in evaluating cloud security. This approach determines if both the vendor and the organization have multiple levels of protections for all data and physical assets. The levels include:

1) Physical security – there should be a procedure in place to protect the physical facility that houses the servers.
2) Network security – the vendor should have 24 hour trained security and network personnel managing the network security. Competence and skill sets of personnel managing the network are crucial.
3) Intrusion detection – the vendor should be capable of detecting intrusion at multiple points within the network.
4) Firewall management – An organization should provide specifics on firewall policies based on their needs. This can add additional levels of security into the organization's specific portion of the cloud.
5) Data encryption – Organizations should have data encryption techniques inside and outside of the cloud.

Bathe, R., Jawale, V., & Jundre, V. (2013). Secure cloud based document management system. *International Journal of Engineering*, *2*(3). Retrieved from http://www.ijert.org/browse/volume-2-2013/march-2013-

edition?download=2559%3Asecure-cloud-based-document-management-system&start=10.

Abstract. The transition towards paperless offices and increasing adoption of electronic transfer of information through emails and other web based content has prompted organizations to have a system which would manage their documents effectively. A cloud based document management system provides a hassle free classification and identity system that tags documents with information. Electronic documents are considered to be the most valuable information assets in enterprises. As the cloud security era is coming, the existing systems need to be upgraded with most cost-effective measures, so a document security management system suitable for cloud security is also designed. With more documents being integrated electronically and transferred as knowledge points, organizations see document management system as an integral tool to handle growing surge of data and respond to audits without heavy burdens to the business.

Credibility. International Journal of Engineering Research and Technology (IJERT) is an international peer-reviewed, online journal published monthly by ESRSA Publication. IJERT covers topics that appeal to a broad readership of various branches of engineering, science and related fields. IJERT is indexed in DOAJ, EBSCO, Google Scholar, Scientific Commons, CiteseerX, getCITED, Index Copernicus and many more (IJERT, n.d.)

Summary. A cloud-based document management system provides an easy process to classify and tag documents with information. The concept of a cloud-based document management system is not new but the use has started gaining momentum and will grow in the future. The cloud-hosted system delivers information via the web, which gives around the clock access to information from any remote location. Cloud enables SaaS providers to enhance their existing offerings by incorporating the flexibility and scalability that cloud storage offers. As noted by the authors, in order to increase trust in cloud computing, there is a need to increase transparency and accountability of data in the cloud for both enterprises and end-users. However, current system tools are unable to log file accesses and transfers effectively within a cloud environment. In this paper, the authors present Flogger, a novel file-centric logger suitable for both private and public cloud environments, designed to provide full transparency of the entire data landscape.

Healey, M. (2010, May 17). Practical guide to SaaS success. *InformationWeek*, (1267), 40.

Abstract. Software as a service is hot, and we have the stats to prove it: Fully 68% of the 530 respondents to our InformationWeek Analytics 2010 Outsourcing Survey use some form of SaaS. And they're happy with that decision. Most say SaaS provided higher-quality results versus internal sourcing, with 37% pointing to the IT nirvana of "higher quality at a lower cost." Forty-four percent plan to expand their use of SaaS this year.

Credibility. Mike Healy is the president of Yeoman Technology Group, an engineering and research firm, and an InformationWeek contributor. Mike has more than twenty-five years of experience in technology integration and business development. He has a BA in operations management from the University of Massachusetts Amherst and an MBA from Babson College. Mike is a contributor to InformationWeek focusing on implementing technology and the impact of internet and cloud technology.

Summary. InformationWeek analytics 2010 outsourcing survey shows 68% of 530 respondents using some form of SaaS. Most of these respondents point to a higher quality with a lower cost. And 44% plan to expand their use of SaaS. While some SaaS providers promise quick turnaround on deliverables in setting up a SaaS, there are some problems to be aware of or at least prepare for. Mike Healey lists the following categories to concentrate on when using a SaaS provider:

- Interconnectivity – Software that needs to be integrated with SaaS should be made simple for all users. If clients are logging into to use software, they should not have to download a trial version just to use the software.
- Vendor management – SaaS can be viewed as another source of outsourcing. Management needs to be able to handle the SaaS vendors as they do with all other vendors.
- Proactive Security – SaaS vendor's agreement holds itself responsible for securing its systems and enforcing any policy restrictions companies provide – the rest falls on the company that is using SaaS.
- Monitoring – Establish performance benchmarks for basic tasks and run them from different connectivity points.
- Business continuity – Since SaaS relies on the connectivity of the internet, there should be connectivity redundancies in place.

Mell, P., & Grance, T. (2011). The NIST Definition of cloud computing. *NIST special publication*, *800*, 145.

Abstract. The purpose of this publication is to provide the NIST definition of cloud computing. NIST intends this informal definition to enhance and inform the public debate on cloud computing. Cloud computing is still an evolving paradigm. Its definition, use cases, underlying technologies, issues, risks, and benefits will be refined and better understood with a spirited debate by the public and private sectors. This definition, its attributes, characteristics, and underlying rationale will evolve over time.

Credibility. The National Institute of Standards and Technology (NIST) is responsible for developing standards and guidelines, including minimum requirements, for providing information security for all federal agency operations and assets. Guidelines are prepared for Federal agencies, but it may be used by nongovernmental organizations as well.

Peter Mell is a senior computer scientist for the National Institute of Standards and Technology (NIST). Peter is a graduate from the University of California with a MS degree in computer science.

Timothy Grance is a senior computer scientist at the National Institute of Standards and Technology (NIST) holding a variety of positions such as group manager, systems and network security and program manager for cyber and network security, and led projects with cloud computing just to name a few. In 2003, he was named to the Fed 100 by Federal Computer Week as one of the most influential people in information technology for the US government (Cloud Security Alliance, n.d.).

Summary. The National Institute of Standards and Technology (NIST) published this report to provide a definition of cloud computing. The intention of this informal definition is to inform and enhance the public debate on cloud computing. The NIST definition of cloud computing is: "Cloud computing is a model for enabling ubiquitous convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models" (Mell & Grance, 2011), p. 2).

Tolliver-Nigro, H. (2009). SaaS 101: The basics of software as a service. *Seybold Report: Analyzing Publishing Technologies, 9*(15), 3–8.

Abstract. The article focuses on the emergence of software as a service (SaaS) which is a software architecture that holds a single data set source and code, and offers application programming interfaces (APIs). It notes that SaaS model manages sales-related applications and has established to embrace all types of business software, from accounting to workflow management. It also points that data security and data integrity must be considered before investing in such architecture.

Credibility. The Seybold report was founded in the 1970s by John Seybold, this newsletter has a long history and a strong tradition of serving its readers by delivering detailed and objective information and reviews of graphic arts technology, as well as informed and intelligent commentary about such technology.

The *Seybold Report* is the definitive and independent source of information about the technologies used for publishing and printing (The Seybold Report, n.d.).

Heidi Tolliver-Nigro is a commercial and digital printing industry analyst, feature writer, columnist, editor, and author for nearly 20 years. Heidi Tolliver-Nigro is currently a paid blogger for *The Inspired Economist* and Wausau Paper's *DigitalSpace* on "green" topics related to print marketing. She is a long-time contributing editor and columnist for *Printing News,* for which she writes two monthly columns: "Personal Effects," which features monthly analysis of 1:1 (personalized) printing case studies, and "Creative Connection," as well as a regular contributor to *The Seybold Report* and *Graphic Arts*

Magazine on topics related to digital and 1:1 printing and leading-edge technologies like QR codes (Tolliver-Nigro, n.d.).

Summary. SaaS is the ability to rent the use of software hosted by a third party. Renting the software will not require the purchase of new hardware or software to support it. The software is used via a web browser and requires no installation of the software. The SaaS vendor is responsible for all maintenance, upgrades and support issues for the software.

The author warns of SaaS vendor failings and some security breaches that have occurred. If a SaaS model is purchased, there are no guarantees of the vendors continued existence. A franchise supplier of print and promotional products, Proforma XTI, is a victim of a SaaS company going out of business and lost all their data that was hosted.

To evaluate the safety and security of a SaaS solution the company needs to understand the SaaS vendor's architecture. Just because a vendor offers software use online does not mean it is a true SaaS vendor. For example, an application service provider (ASP) will focus on building clients services on one server only. Once the clients get to a critical mass and the service starts to slow down, then the ASP vendor will create another server and transfer clients to that server only. True SaaS is multi-tenant. Multi-tenant means the architecture is properly created to support many people in accessing their information at the same time in one server. The SaaS vendor runs the product on a single instance, on multiple machines using a single data set source. In addition, if these servers reach their bandwidth max, other servers turn on and support the service in the same way automatically.

Security it set to the highest levels and many meet government security standards. SaaS companies may have more knowledge in security than regular companies do since their focus is to protect their clients' data. SaaS providers also have more experience with internal security and restrict access to their employees in accessing information and have procedures in place for monitoring.

When choosing a SaaS provider, do your due diligence on a trustworthy supplier:

- Make sure it's a true SaaS solution and not a ported application service provider (ASP) solution.
- Understand what your organization needs in terms of data security, back-up, and recovery needs. This will help the SaaS vendor meet those needs.
- Involve IT to tour the data center of the SaaS provider and to talk to engineers.
- Get references.

The outlook for SaaS is promising. In 2008, the SaaS market reached a revenue of $6.6 billion and with consistent growth it will reach $16 billion in 2013. Not just large and international business are adopting SaaS, small and medium size business are using SaaS as well.

The following set of reference provides current definitions of EDRMS.

Alalwan, J., & Thomas, M. (2011). An ontology-based approach to assessing records management systems. *E-Service Journal, 8*(3), 24.

Abstract. Organizations seek to improve their records management (RM) systems to improve efficiency and meet legislative requirements. To achieve these two goals, evaluation of RM, which is normally done manually, is a necessity for every firm. In this paper, we design and evaluate an ontology that will help in evaluating RM systems. Building the ontology will be the first step in developing an ontology-based RM evaluation system. We argue that the proposed ontology-based RM evaluation system has promising features and benefits. Using this ontology will raise the efficiency of the evaluation process and facilitate sharing and communication of evaluation results.

Credibility. E-service Journal publishes regular research articles and shorter articles including reviews, outlooks, and responses. Papers submitted for publication must be original, previously unpublished, and not under consideration for publication elsewhere. All submissions undergo a review process (JSTOR, n.d.)

Project Muse is a leading provider of digital humanities and social sciences content; since 1995, its electronic journal collections have supported a wide array of research needs at academic, public, special, and school libraries worldwide. MUSE books and journals, from leading university presses and scholarly societies, are fully integrated for search and discovery, (Project MUSE, n.d.).

Summary. This paper discusses an ontology approach which will help in evaluating records management (RM) systems. The authors believe that the rigorous organization of RM knowledge is the best approach in evaluating RM systems. The authors define ontology as formal and explicit specifications of a shared concept.

According to ISO 15489-1, records management (RM) is defined as “the field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including the processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records” (Alalwan & Thomas, 2011).

The three major criteria that RM evaluation generally aims to reach are:

- The legislative requirements that the organization needs to follow;

- The standards, policies, and procedures regarding records that are related to those specific requirements;
- The training courses that may increase employee efficiency.

To identify the main concepts of the RM assessment model, the authors conducted a detailed review of the three most popular RM evaluation guidelines:

- Australian assessment tool check-up from the National Archives of Australia;
- British evaluation workbook and methodology;
- Records Management self-evaluation guide from the U.S. National Archives and Records Administration.

All three guidelines showed similarities in their concepts. The author's state this could be attributed to the human involvement required in interpretation of the guidelines.

An electronic records management (ERM) ontology is in introduced to show overlap and concept relationships are similar in the above guidelines. To understand the ERM, the records management system is defined as having a type of records to identify all organizational records that are classified as paper, electronic, and online records. An ontology-based system can help users share knowledge, and facilitate common understanding of the RM domain.

Empel, S. (2012). How to evaluate new technologies for RIM impact. *Information Management Journal*, *46*(6), 36–40.

Abstract. The article focuses on evaluation of the effect of new technology on the records and information management (RIM). It states that adoption of technology could create RIM-related risks that need to be addressed before the acquisition of the record-keeping system technology for effective information governance. It says that RIM professionals must develop goals where technologies should be aligned such as systems strategy, technical strategy, and acquisition strategy. It mentions the application of Generally Accepted Recordkeeping Principles (R) for the evaluation of technologies which include accountability, transparency, and protection of records and information.

Credibility. Sofia Empel, is president of Records Update, a women business enterprise (WBE) certified company which provides professional consulting and information and records management support services to corporations, law firms, universities, not for profits, and government organization. Sofia is a member of the Association of Records Managers and Administrators (ARMA), Association for Information and Image Management (AIIM), and many other reputable associations. Sofia has a Bachelor's in business administration, Master's in library and information science. She is also a certified records manager (CRM), certified document imaging architect (CDIA+) (Records Update, n.d.).

Summary. New technologies are introduced to support records and information management (RIM) professionals to promote efficiency, increased productivity, and reduced costs. RIM professionals must evaluate risks by conducting comprehensive evaluations during the planning stages to acquire the new technology. According to Empel (2012), a strategically aligned plan is needed for RIM goals when introducing new technology. The different strategies outlined are:

- Systems strategy – This strategy provides a plan and detail on how specific technologies fit into the organization.

- Acquisition strategy – Acquisition decisions should be based on business needs, recordkeeping capabilities, and whether the new technology can evolve with the business.
- Technical strategy – Technical requirements vary on a case-by-case basis, but some considerations include hardware, software, platform, connectivity, administration, support, and maintenance.

New RIM technologies should align with the generally accepted recordkeeping principles (GARP), while supporting business objectives through standard records management processes.

State Records NSW. (n.d.). Record keeping in brief 61 - FAQs about EDRMS. Retrieved April 30, 2013, from http://www.records.nsw.gov.au/recordkeeping/government-recordkeeping-manual/guidance/recordkeeping-in-brief/recordkeeping-in-brief-61#what-is-an-edrms-

Abstract. And EDRMS is defined by the State Records of New South Wales (NSW) as "an electronic document and records management system. It is an automated software application designed to facilitate the creation, management, use, storage and disposal of a range of both physical and digital documents and records in an integrated way. An EDRMS may also automate business processes such as workflows and approvals and be integrated with other business systems" (State Records NSW, n.d.).

Credibility. State Records is the New South Wales Government's archives and records management authority.

Summary. An EDRMS combines document management and records management functionality. EDRMS can bring the following benefits to an organization:

- Facilitate the move from paper to digital records
- Improve business efficiency and productivity
- Security of documents
- Provide accountability and transparency for compliance
- Enable to provide recordkeeping at a large scale.

When considering moving to an EDRMS, an assessment should be made to take into consideration the company's information architecture, current business systems, recordkeeping culture, review policies and procedures, and understand the existence and current use of information and recordkeeping tools.

Nguyen, L. T., Swatman, P. M. C., & Fraunholz, B. (2007). EDMS, ERMS, ECMS or EDRMS: Fighting through the acronyms towards a strategy for effective corporate records management. *ACIS2007 Toowoomba 5 to 7 December 2007 [electronic resource] : proceedings of the 18th Australasian conference on information systems*, 790–800.

Abstract. Records management has been receiving increased attention around the world over the last two decades as governments issue ever more laws and regulations about the management of corporate records. An electronic system to manage records effectively is the ultimate goal of every organisation in both the public private sectors – whether to support the development of E-Government or to conduct business legally. Such systems are not yet clearly defined, however, as the obvious confusion and inconsistency of nomenclature makes very clear. This paper highlights the problem and calls for research into this essential but currently ignored area.

Credibility. This article was written for the Australasian conference on information systems (ACIS). This event is held annually for information systems and information technology professionals and academics (Australasian Conference on Information Systems, 2013). ACIS is the premier conference in Australasia for information systems covering technical, organizational, business and social issues in information technology to real world problems (Australasian Conference on Information Systems, 2013).

Paula Swatman, one of the authors of this article, is an adjunct professor at the University of Tasmania in Australia. Paula's academic specialties include: cloud computing & mobile access; researcher in enterprise networking, and organizational system and structure transformation (Swatman, n.d.).

Bardo Fraunholz is a program director for the school of Information and Business Analytics, Deakin University. Bardo lectures in project management, enterprise modeling and business information communication systems. Bardo has a Master's in Information Systems/Accounting from Germany and a post-graduation in legal studies specializing in IT, media and corporate law from London (Fraunholz, n.d.).

Summary. The paper investigates the current status of a variety of approaches to corporate recordkeeping systems. The authors first define records management in Australia as "the making and maintaining of complete, accurate and reliable evidence of business transactions in the form of recorded information" (Nguyen, Swatman, & Fraunholz, 2007, p.791). Other records management definitions are listed from the United Kingdom and the United States to show similarities. Nguyen, Swatman, & Fraunholz (2007) set to identify the different software solutions under the many acronyms such as ECM, EDRM, EDM, ERM, and EKM. These acronyms or categories are derived from the software vendors themselves. The State Records of South Australia (SRSA) established a panel to provide technical standards for electronic document and records management solutions which meet the South Australian Government's recordkeeping standards. While the functional requirements are detailed, the software vendor's features are broad. Software vendors do not appear to have identified any unambiguous functionality that would distinguish, for example, records management from document management. Organizations faced with a decision based on vendor offerings have little external information to measure against or a simple label to identify the adequacy of the system. For South Australia, the useful information available in purchasing an enterprise records management solution would point to the functional compliance requirements for EDRMS developed by State Records.

The following set of references address potential strengths, weaknesses, opportunities, or threats (SWOT) related to cost when using SaaS in support of an EDRMS.

Berg, K. (2011). Federal Government enters the era of the "Cloud." *News Media & the Law*, *35*(4), 16–18.

Abstract. The White House and the Office of Management and Budget (OMB) have for a few years been encouraging agencies to reap the benefits of the new technology, and many federal offices have already begun a migration to the cloud.

Credibility. The *News Media and the Law* is published by The Reporters Committee for Freedom of the Press. For more than 40 years, the Reporters Committee for Freedom of the Press has provided free legal advice, resources, support and advocacy to protect the First Amendment and Freedom of Information rights of journalists working in areas where U.S. law applies, regardless of the medium in which their work appears. Funded by corporate, foundation and individual contributions, the Reporters Committee serves more than 2,000 reporters, editors and media lawyers who call for help each year, as well as the tens of thousands who use its website (Reporters Committee for Freedom of the Press, n.d.).

Summary. The Federal Government is transitioning their records management duties to the cloud along with some other services such as e-mail. An assessment conducted in 2010 by the National Archives and Records Administration (NARA) found that 95% of federal agencies self-reported that they were at moderate or high risk of essentially losing records. The same assessment identified electronic records from employee e-mail to basic data, as one of the troubling issues the federal agencies faced. As the federal agencies struggle to preserve terabytes of government records, the solution proposed is cloud computing.

The Chief Information Office (CIO) in 2009, Vivek Kundra, unveiled an ambitious plan to overhaul the government's lagging computer technology, designed to help government by cutting the need for managing the government's vast amount of data on expensive, aging, energy inefficient, in house servers. This plan is expected to save the government billions in IT costs over a ten-year migration plan. One example of an aging infrastructure is when the Federal Government initiated the cash for clunkers program, the website crashed because the government failed to predict the response that overloaded their capacity.

A cloud first initiative has been started within the government agencies and states that the cloud should be the default whenever secure, reliable, cost-effective cloud options exist.

Records management in the cloud will be a big focus for the government since the agencies will need to fulfill their legal responsibilities to maintain important information ranging from correspondence to scientific databases, and ensuring they are accessible when requested by the public or the courts. NARA crafted a legal language they thought agencies should use when signing up with cloud vendors. This language includes clear guidelines on record-keeping requirements the government needs. The records the government preserves have to be organized, follow disposition schedules, and be assessable.

Bibi, S., Katsaros, D., & Bozanis, P. (2012). Business application acquisition: On-premise or SaaS-based solutions? *IEEE Software*, *29*(3), 86–93. doi:10.1109/MS.2011.119

Abstract. The benefits of migrating business software applications to the cloud are a dominant IT topic among consultants, software managers, and executives. The broad interest in cloud computing is motivated by the prospect of quick, painless deployment and maintenance of applications that are now a burden of the enterprise. The authors propose an analytical method for deciding whether the features and cost of a cloud solution are appropriate to the business IT problem and whether the risks are reasonable and manageable.

Credibility. Stamatia Bibi is a contracted lecturer at the University of Western Macedonia and a research collaborator at Aristotle University of Thessaloniki, where she performed the work reported in this article. Her research interests include software process models, estimating software development cost and quality, cloud computing, and open source software. Bibi has a PhD in informatics from Aristotle University of Thessaloniki (Bibi, Katsaros, & Bozanis, 2012)

Dimitrios Katsaros is a lecturer with the Department of Computer and Communication Engineering at the University of Thessaly. His research interests are in the area of distributed systems. Katsaros has a PhD in informatics from Aristotle University (2004). He's coeditor of *Wireless Information Highway*s (IRM Press, 2005) (Bibi, Katsaros, & Bozanis, 2012).

Panayiotis Bozanis is an assistant professor at the University of Thessaly. Bozanis has a PhD in computer engineering and informatics from the University of Patras. He's co-editor of *Advances in Informatics* (LNCS 3746, Springer, 2005) and a member of the European Association for Theoretical Computer Science (Bibi, Katsaros, & Bozanis, 2012).

Summary. The authors create a method to support a decision whether an enterprise should continue operating its own business software on site or subscribe to a hosted SaaS service. The model takes into account software costs estimations, information system cost models, service level agreements (SLA), and popular billing methods. One such popular billing model includes a fixed price or price per user per month. The model aims to assist practitioners gather all economic aspects of an IT deployment model to produce total cost of ownership (TCO) estimates. The model is based on three types of costs that companies can combine to use TCO which are up-front costs, annual divestment costs, and operational costs with regards to SaaS.

Up-front costs are labeled as Cu. Other labels are added to create the model. Cu represents the investment costs of adoption a new software system. It includes costs associated with the software, such as development (Cd), subscription (Csaas_sub), integration and customization costs (Cin), user training (Cut), and operational costs (Co).

The following equation is used to calculate up-front costs (Cu) where N represents the number of users subscribing to a SaaS application: Cu(SaaS) = N x Csaas_sub + Cin + Cut + Co.

Annual divestment costs are labeled as Cad. This second cost type includes relevant annual costs necessary to preserve the operation of the existing software system. Customization (Ca_cust) and professional support (Ca_ps) costs are introduced to the model. The following equation is used to calculate annual divestment costs (Cad): Cad (saas) = N x Csaas_sub + Ca_ps + Ca_cust.

Operational costs are labeled as Co. The following equation is used to calculate operational costs (Co): Co(saas) = Cic (internet connection costs).

The authors use the above model in a case study of a company with 2,300 employees. The total cost of ownership shows large savings in SaaS use between the first and tenth year. At year twenty the costs differences start to compare with costs in keeping the software and infrastructure in-house.

Foley, J. (2012, October 22). Expect to save millions in the cloud? Prove it. *InformationWeek*, (1347), 5.

Abstract. The article offers the author's view on the efforts of the U.S. General Services Administration (GSA) in saving money through cloud computing. He mentions its adoption of cloud computing services from Google Inc. to meet its projected cost savings of $15 million. He also considers the experience of the agency as a reminder of the significance of business planning and project management.

Credibility. John Foley is an Editor of InformationWeek Government, started his career as a tech journalist inside the Washington beltway, covering the breakup of AT&T and the deregulation of the telecom industry. John has held a variety of writing and editing positions with InformationWeek, including serving as the magazine's Editor. His areas have included open systems, databases, business intelligence, and Microsoft, and he now leads InformationWeek's expanded editorial coverage of technology implementation and strategy in federal, state, and local government (InformationWeek, n.d.).

Summary. The U.S. General Services Administration (GSA) moved to implement Google's cloud services for email and collaboration. The GSA projected it would save $15 million over five years. Findings from an internal audit review reveal that there is not enough evidence of those projected savings.

The audit showed the projected cost savings couldn't be verified. In addition, performance measures were lacking. GSA did not create an inventory of the applications being moved to the cloud prior to upgrading to Google's service. But still the GSA stands by the estimated cost savings of $15 million over five years.

The GSA situation is a reminder of the importance of business planning and project management at the start cloud computing projects. There is no guarantee that the cloud will be cheaper than in-house built IT. According to interviews conducted by the author, there are not many IT people in the Government that know how much things cost. Federal IT professionals are still learning how to build a cloud business solution that can hold up to scrutiny.

Hai, H. , Sakoda, S. , & Fujitsu, L. (2009). SaaS and integration best practices. *Fujitsu Scientific & Technical Journal, 45*(3), 257-264.

Abstract. The rising adoption of software-as-a-service (SaaS) applications by enterprise organizations has been driven by deep dissatisfaction with on-premise applications, which require organizations to purchase and deploy infrastructure, overstock on licenses, and pay for expensive resources for customizations, upgrades, and on-going maintenance. The large upfront investments combined with unpredictable costs and immeasurable returns on investment have prompted organizations to seek cheaper less-risky alternatives. Many have found that SaaS applications, which require minimal or no infrastructure and maintenance, can be deployed quickly and have a predictable cost model representing less risk and a faster return on investment. The new demand has led to rapid innovation in SaaS applications, SaaS platforms, third-party SaaS add-ons, and SaaS integration tools. However, enterprise organizations still have the burden of integrating these applications with their back-office systems and on-premise applications, without which the SaaS applications have little to no value. Complex enterprise integration requirements challenge even the best SaaS solution providers today; there are still limitations and pitfalls to be wary of. In this paper, we describe some SaaS integration best practices, present a case study, and highlight emerging integration technologies that can help ease the burden of integrating SaaS applications.

Credibility. Fujitsu Scientific & Technical Journal is published quarterly by Fujitsu Limited to introduce the Fujitsu group's research and development activities, products, and solution services **(**Fujitsu Global, n.d.).

Henry Hai received a BS degree in Computer Science and Philosophy from Rensselaer Polytechnic Institute, New York, USA in 1996. He joined the SaaS practice of Fujitsu Consulting Inc. in October 2003 and has been engaged in implementing and integrating Saas applications for enterprise customers (Hai, Sakoda, & Fujitsu, 2009).

Seitar Sakoda received a BS degree in Physics from Kyoto University, Kyoto, Japan in 1998 and a MS degree in Physics from the University of Tokyo. He focuses in system development, technology support, and technical consulting (Hai, Sakoda, & Fujitsu, 2009).

Summary. This paper provides some SaaS integration best practices in order to help ease the burden of integrations. Most applications are not designed for flexibility, and unexpected costs can arise when supporting the infrastructure that maintains these applications are causing constrains to the business instead of enabling it. SaaS is introduced in order to release some of that burden. SaaS solution providers take responsibility for managing the applications, security, performance, availability, reliability, and scalability for the application service. SaaS enables costs savings since the software is shared by multiple tenants (multi-tenancy) applied to all tiers of the software architecture. All tenants share the same codebase and instances of the application which enables the provider to provide it at large economies of scale. The economies of scale are savings are passed on to customers through a low-cost pay-as-you-go subscription model. Adding to the cost savings, the pay-as-you-go model has the benefit of permitting customers to regard the cost as an operating expense rather than a capital expense, which allows all the financial risk to be taken over an extended period of time instead of up front.

Integration is critical to the success of any application. Fujitsu consulting has developed a five-stage methodology for SaaS implementation which includes: define, discover, design, develop, and deploy.

Integration costs can be controlled if application programming interfaces (API) published by the SaaS provider are used, but still the cost of integration can be 30%-45% of the overall SaaS implementation. Many of the larger traditional on-premise integration vendors such as IBM DataStage, Informatica, and AB Initio already offer specialized connectors for SaaS applications. These connectors can significantly reduce the integration effort.

Defining performance metrics is the key to success of the project and can help define how the integration is designed and implemented. Knowing the initial size and growth of the SaaS application data is necessary to ensure that the organization will not exceed its data storage limits and incur additional costs.

There are cloud-to-cloud integrations that are available which are called integration-on-demand. These services allow non-technical users to customize and deploy customized integrations through menu driven wizards. The pricing model for integration-on-demand is flexible and affordable compared to their on-premise counterparts.

SaaS solution providers are starting to focus on pre-built integrations. This will help reduce the cost and complexity of integrations. SaaS has not dramatically reduced the complexities of integration with SaaS applications; organizations still have to deal with vendor specific API's or connectors that offer different capabilities. System integrators will still play a key role when integrating SaaS with on premise solutions.

Herbert, L., Erickson, J. (2011). The ROI of cloud apps. *Forrester Research*. Retrieved from https://www.mercurymagazines.com/pdf/BOXNET3.pdf

Abstract. Cloud applications continue to gain momentum in enterprise applications as buyers are attracted to fast deployment speeds, low upfront costs, and ongoing flexibility to scale up or down as needs change. But as firms spend more and more of their closely guarded IT dollars on cloud applications, sourcing executives must scrutinize the long-term value of these investments. Today's cloud investments represent millions of dollars of annual IT spend for some larger consumers of cloud. This report analyzes the longer-term, five-year cost of ownership and value for cloud applications across four categories: customer relationship management (CRM), enterprise resource planning (ERP), collaboration (including email), and IT service management.

Credibility. Liz Herbert is a featured speaker at leading industry events such as SaaScon, Nascom, Society of Information Managers, and the World BPO Forum. Liz has been quoted in leadings publications that include The Wall Street Journal, Fortune, The New York Times, and CIO Magazine. Additionally Liz has been feature as an expert in software-as-a-service (Saas) on TV news segments, including Boston-based NECN, and was recognized as he IIAR Services analyst of the year for 2010 (Forrester Research, n.d.) (a).

Jon Erickson is the director of Forrester's Total Economic Impact (TEI) practice. Jon's focus over the past fourteen years at Forrester has been on developing methodologies for measuring and communicating the value of technology to IT strategy and planning executives (Forrester Research, n.d.)(b).

Forrester Research is a global research and advisory firm serving professionals in 13 key roles across three distinct client segments. Forrester clients face progressively complex business and technology decisions every day. To help clients understand, strategize, and act upon opportunities brought by change, Forrester provides proprietary research, consumer and business data, custom consulting, events and online communities, and peer-to-peer executive programs. Forrester guides leaders in business technology, marketing and strategy, and the technology industry through independent fact-based insight, ensuring their business success today and tomorrow (Forrester, n.d.).

Summary. This report analyzes the longer term cost of ownership and value for cloud applications. Cloud applications continue to gain in popularity as these solutions provide lower entry costs and fast speeds of deployment. According to the authors, few understand its full implications. Organizations implementing cloud applications can expect the following:

- Ongoing subscription costs. The ongoing cost is the rental fee for using the applications which most often is per month or per usage-based. Criteria to calculate costs include storage (i.e., number of documents) or throughput (number of transactions processed.
- Vendor management. Cloud applications require focus on contracting, managing, service level agreements (SLA's), and performance management. Contract dates can vary widely and would require the organization employing SaaS to constantly monitor and manage vendors.
- Cloud orchestration costs. Cloud vendors do not usually provide a suite of applications that an organization can use. Most cloud solutions focus on a specific module. Organizations can wind up dealing with a lot of different applications from different vendors. This multivendor environment can lead to additional costs like integrations, end user support, upgrade management, testing and workflow.

Contract negotiation strategy can increase the value of cloud applications. Organizations should consider planned usage to determine the right deal length. If a large investment is made on SaaS, then the contract with the SaaS vendor should favor a longer time frame. If a company is growing fast, then perhaps a shorter deal should be favored in order to provide leeway to change course.

Other strategies that can assist in getting the best value out of the cloud include options such as enterprise wide license options that avoid strict per user-based pricing. Hidden costs can mostly be avoided if an organization tries to understand their planned usage as best as possible from the beginning. Some cloud contracts won't include items such as mobile access, or test environments. Knowing these needs from the beginning will help with negotiations.

Tak, B. C., Urgaonkar, B., & Sivasubramaniam, A. (2013). Cloudy with a chance of cost savings. *IEEE Transactions on Parallel and Distributed Systems, 24*(6), 1223–1233. doi:10.1109/TPDS.2012.307

Abstract. Cloud-based hosting is claimed to possess many advantages over traditional in-house (on-premise) hosting such as better scalability, ease of management, and cost savings. It is not difficult to understand how cloud-based hosting can be used to address some of the existing limitations and extend the capabilities of many types of applications. However, one of the most important questions is whether cloud-based hosting will be economically feasible for my application if migrated into the cloud. It is not straightforward to answer this question because it is not clear how my application will benefit from the claimed advantages, and, in turn, be able to convert them into tangible cost savings. Within cloud-based hosting offerings, there is a wide range of hosting options one can choose from, each impacting the cost in a different way. Answering these questions requires an in-depth understanding of the cost implications of all the possible choices specific to my circumstances. In this study, we identify a diverse set of key factors affecting the costs of deployment choices. Using benchmarks representing two different applications (TPC-W and TPC-E) we investigate the evolution of costs for different deployment choices. We consider important application characteristics such as workload intensity, growth rate, traffic size, storage, and software license to understand their impact on the overall costs. We also discuss the impact of workload variance and cloud elasticity, and certain cost factors that are subjective in nature.

Credibility. *IEEE Transactions on Computers* (*TC*) is a scholarly archival journal published monthly with a wide distribution to researchers, developers, technical managers, and educators in the computer field. It publishes papers, brief contributions, and comments on research in areas of current interest to the readers. These areas include, but are not limited to, the following: (a) computer organizations and architectures; (b) operating systems, software systems, and communication protocols; (c) real-time systems and embedded systems; (d) digital devices, computer components, and interconnection networks; (e) specification, design, prototyping, and testing methods and tools; (f) performance, fault tolerance, reliability, security, and testability; (g) case studies and experimental and theoretical evaluations; and (h) new and important applications and trends. ISSN 0018-9340 **(**IEEE Transactions on Computers, n.d.).

Byung Chul Tak received his MS degree in computer science from Korea advanced Institute of Science and Technology (KAIST) in 2003, and a PhD degree in computer science in 2012 from Pennsylvania State University. He is currently a research staff member at IBM T.J. Watson Research Center. He is a recipient of the University Graduate Fellowship (UGF) of the Pennsylvania State University in 2006 and the IBM PhD Fellowship in 2010 (Tak, Urgaonkar, & Sivasubramaniam, 2013).

Bhuvan Urgaonkar received his MS and PhD degree in computer science at the University of Massachusetts, in 2002 and 2005, respectively. He is an associate professor in the Department of Computer Science and Engineering at the Pennsylvania State University. He is a recipient of the US National Science Foundation (NSF) CAREER Award, research awards from HP Labs and Cisco, and has coauthored best student papers at IEEE MASCOTS 2008 and ICAC 2005 conferences (Tak, Urgaonkar, & Sivasubramaniam, 2013).

Anand Sivasubramaniam received the BTech degree in computer science from the Indian Institute of Technology, Madras, in 1989, and the MS and PhD degrees in computer science from the Georgia Institute of Technology in 1991 and 1995, respectively. He has been on the faculty at The Pennsylvania State University since fall 1995, where he is currently a professor. His research interests are in computer architecture, operating systems, and performance evaluation. His research has been funded by the US National Science Foundation (NSF) through several grants, including the CAREER award, and from industries including Google, IBM, HP, Microsoft, Seagate, and Unisys Corp. He has several publications in leading journals and conferences, has been on the editorial boards of IEEE Transactions on Parallel and Distributed Systems and IEEE Transactions on Computers, and has served on several conference program committees. He is a fellow of the IEEE and an ACM Distinguished Scientist (Tak, Urgaonkar, & Sivasubramaniam, 2013).

Summary. Cloud based solutions have some known positive factors in use. Cloud based solutions offer ease of management since the cloud provider assumes management related responsibilities such as procurement, upgrades, and maintenance of hardware and software. Cloud use also offers capital expenditure savings and operation expenditure savings by eliminating the need to purchase infrastructure and elimination of additional staffing related costs.

Not all cloud use will have the same savings for everyone, and some may not even offer savings in the end. One example is if an organization has pre-existing infrastructure, it won't benefit much from a low cost entry barrier for cloud services since they already have their infrastructure in place. Also the best approach for some organizations may be a hybrid approach where a combination of public cloud and in house systems are used. Another example is the question of how much effort and cost is involved in migrating current applications to the cloud?

The authors use a set of metrics in order to analyze the cost of various cloud hosting scenarios:

- Identification and classification of cost contributors (quantifiable, less quantifiable, direct costs, and indirect costs).
- Identification of deployment choices (pure in-house, pure cloud, hybrids).
- Case studies of Net Present value (NPV) based cost analysis.

  To provide the analysis, the authors chose to use two prominent cloud providers in Amazon and Microsoft. The following five hosting options were analyzed and the cloud focus has been to discuss the public cloud:
- Fully in-house applications

- Fully IaaS – Amazon EC2 cloud
- Amazon EC2 (IaaS) + Amazon RDS (SaaS)
- In house + Amazon RDS (SaaS)
- In house + Microsoft SQL Azure (SaaS)

The authors studied the critical factors such as workload intensity, growth rate, data transfer sizes, storage capacity, and software licensing. For example, in a specific intended operational period, a medium and stagnant growth company of three years, the best hosting options would be to go Fully EC2 (IaaS). If a cloud operation is chosen to run for eight years, then a fully in house choice is preferred. It seems that for smaller workloads, the cloud based options are suited for operational period based on intensity and growth rate.

Storage capacity and software licenses show that substantial cost would be used in a fully in-house system based on high storage demands (4.5TB). With a full EC2 system, renting storage is cheaper than the cost of making significant investments in high-end RAID storage.

Workload-based partitioning shows the in-house cost in an increasing pattern because the server capacity increases incrementally. The cloud cost shows a decreasing function because an application in the cloud can grow and shrink to match workload.

Licensing fees can be lowered by using pay-per-use SaaS DB by eliminating SQL server licenses fees shown in their study. SaaS options can be cost effective for applications will a high software license maintenance fee.

There are a large number of variables and complexities when migrating to the cloud. Overall the authors find that complete migration to today’s cloud is appealing only for small/stagnant businesses; component based partitioning options are expensive due to high costs of data transfer; and workload-based partitioning options can offer the best of in-house and cloud deployment for certain applications.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing - The business perspective. *Decision Support Systems, 51*(1), 176–189. doi:10.1016/j.dss.2010.12.006

Abstract. The evolution of cloud computing over the past few years is potentially one of the major advances in the history of computing. However, if cloud computing is to achieve its potential, there needs to be a clear understanding of the various issues involved, both from the perspectives of the providers and the consumers of the technology. While a lot of research is currently taking place in the technology itself, there is an equally urgent need for understanding the business-related issues surrounding cloud computing. In this article, we identify the strengths, weaknesses, opportunities and threats for the cloud computing industry. We then identify the various issues that will affect the different stakeholders of cloud computing. We also issue a set of recommendations for the practitioners who will provide and manage this technology. For IS researchers, we outline the different areas of research that need attention so that we are in a position to advice the industry in the years to come. Finally, we outline some of the key issues facing governmental agencies who, due to the unique nature of the technology, will have to become intimately involved in the regulation of cloud computing.

Credibility. This article was published by Elsevier for the Decision Support Systems Journal. Elsevier is a publishing company that publishes medical and scientific literature (Elsevier, 2013).

Sean R. Marston is a PhD candidate in the Department of Information Systems and Operations Management in the Warrington College of Business Administration at the University of Florida. He holds a BE in Computer Engineering and an MBA from Georgia Institute of Technology. His current research is in the area of digital distribution, ecommerce, and cloud computing (Marston, Li, Bandyopadhyay, Zhang, & Ghalsasi, 2011).

Zhi Li is currently a PhD student in the department of Information Systems and Operations Management in the University of Florida, Gainesville. His research interests include economics of Information Systems; Artificial Intelligence and Data Mining; Systems Analysis and Design; and Electronic Business (Marston, Li, Bandyopadhyay, Zhang, & Ghalsasi, 2011).

Subhajyoti Bandyopadhyay is an Associate Professor in the department of Information Systems and Operations Management in the University of Florida, Gainesville. He received his PhD in MIS from Purdue University in 2002. His work has been published in several journals in the areas of Information Systems, Operations Management and Marketing. His current research interests include economics of information systems and information systems policy issues, especially in the area of Net Neutrality, national broadband policy and health informatics (Marston, Li, Bandyopadhyay, Zhang, & Ghalsasi, 2011).

Juheng Zhang is a PhD student at the Department of Information Systems and Operations Management at University of Florida. She has previously published in Decision Support Systems. Her research interests are data mining, cloud computing, and quantum computing (Marston, Li, Bandyopadhyay, Zhang, & Ghalsasi, 2011).

Anand Ghalsasi is the Senior Director of Strategic Relationships at Persistent Systems, an award-winning independent software vendor that has developed several cloud based applications with IBM, Microsoft, Oracle, Google and other global technology firms (Marston, Li, Bandyopadhyay, Zhang, & Ghalsasi, 2011).

Summary. This article uses a SWOT analysis for the cloud computing industry with a focus on business related issues.

The following are key advantages to cloud computing:

- Dramatically lowers the cost of entry for smaller organizations trying to benefit from the same business level processing that bigger organizations have. For example, this enables countries that have been so far left behind in the IT service industry to enable full IT services.
- Almost immediate access to software and hardware resources without any upfront capital investments for the organization.
- Cloud computing can lower IT barriers to innovation. An example of companies that use the cloud for their businesses are startups such as Facebook, YouTube, TripIt, and Mint.
- Cloud computing makes it easier for organizations to scale their own services. Cloud allows the resources to be increased up or down depending on demand.
- New class of applications is now possible that deliver real time data to and from mobile applications. Applications that respond in real time to provide information to users.
- Ability to request more computing resources on the fly.

Three core technologies exist for cloud computing: virtualization, multitenancy, and Web services. Virtualization is the technology that hides the computing platform from users but creates and emulated computing platform. Multitenancy is where a single instance of an application servers multiple clients on one server. A Web service is defined by W3C as "a software system designed to support interoperable machine-to-machine interaction of a network. Web services make it easier for a software client to access server applications over a network by standardizing the interfaces between applications.

Some weaknesses of the cloud include:

- Providers are unable to provide an exact location of a client's data. Some organizations, such as in Europe, require constant audits under strict data regulations.
- Large organizations will be reluctant to place their mission critical application to the cloud.

Some opportunities of the cloud are:

- Helps developing countries reap the benefits of information technology without the large upfront costs.
- Small business represents a huge opportunity because small businesses can now use high-end applications that were only available to bigger rivals.
- Mashups can create another opportunity by combining data from two or more external sources to create a new service.

Some threats of the cloud are:

- IT departments may view cloud computing as a threat to their jobs;

- Concerns about the cloud provider going into bankruptcy;
- Lack of standards inhibits some organizations to move to the cloud because global governments have not addressed cloud computing standards directly.

General purpose applications like MS office, e-mail, and collaboration technologies are obvious first applications to start moving to the cloud since these types of applications are not specific only to the organization.

Current cloud computing services are not ideal for larger enterprises, especially if the enterprises have already scaled down their computing operations, although larger enterprises can still benefit from cloud computing by using some of the core technology components of the cloud, i.e. virtualization.

Shum, W. (2013, January 8). State of Oregon embraces HP TRIM for statewide cloud-based records management program.). *Reuters*. Retrieved from http://www.reuters.com/article/2013/01/08/ca-hp-trim-autonomy-idUSnPnSF38775+160+PRN20130108

Abstract. State of Oregon has selected HP TRIM as the cornerstone of a cloud-based records management system that will allow state, city and county agencies to manage, secure and provide access to digital and physical documents. Called Oregon Records Management Solution (ORMS), the cloud-based system is the result of a unique public-private collaboration between Autonomy, Chaves Consulting and Arikkan, utilizing HP TRIM to implement the first statewide electronic records management solution of its kind in the country. ORMS implements HP TRIM in the cloud as part of a Software-as-a-Service solution to make access to government records easier, more transparent, and affordable.

Credibility. Thomson Reuters markets itself as the world's leading source of intelligent information for businesses and professionals. Reuters provides information to the world's businesses and professionals, serving four primary customer groups (Financial & Risk, Legal, Tax & Accounting, and IP & Science) (Thomson Reuters, n.d.).

Summary. The state of Oregon has partnered with Autonomy to use HPTRIM for a cloud-based SaaS records management system that will allow state, city and county agencies to securely manage and provide access to their digital and physical documents. The cloud-based system is called Oregon Records Management Solution (ORMS) and will be a first of its kind to run statewide.

Before using HP TRIM, Oregon employees had to work through back-up tapes, e-mails, and file servers to satisfy requests from the public. With HP TRIM, such requests now take only a matter of seconds to fulfill. For example, a request for 80,000 e-mails generated by the Secretary of State since taking office, took 90 seconds to complete instead of taking days. Because ORMS is cloud-based, there are no up-front infrastructure costs and much lower costs on equipment, power and facilities expenses.

West, D. M. (2010). Saving money through cloud computing. *Governance Studies at Brookings*. Retrieved from http://www.brookings.edu/~/media/research/files/papers/2010/4/07-cloud-computing-west/0407_cloud_computing_west.pdf

Abstract. The U.S. federal government spends nearly $76 billion each year on information technology, and $20 billion of that is devoted to hardware, software, and file servers (Alford and Morton, 2009). Traditionally, computing services have been delivered through desktops or laptops operated by proprietary software. But new advances in cloud computing have made it possible for public and private sector agencies alike to access software, services, and data storage through remote file servers. With the number of federal data centers having skyrocketed from 493 to 1,200 over the past decade (Federal Communications Commission, 2010), it is time to more seriously consider whether money can be saved through greater reliance on cloud computing.

Credibility. Darrell M. West is the vice president and director of Governance Studies and Director of the Center for Technology Innovation at the Brookings Institution. His current research focuses on technology, mass media, campaigns and elections, and public sector innovation. He is the winner of the American Political Science Association's Don K. Price award for best book on technology (for *Digital Government*) and the American Political Science Association's Doris Graber award for best book on political communications (for *Cross Talk*). He has published more than three dozen scholarly articles in a wide range of academic journals, including the American Political Science Review, American Journal of Political Science, Journal of Politics, Public Administration Review, Political Science Quarterly, Social Science Quarterly, the British Journal of Political Science, New England Journal of Medicine, and Urban Affairs Review (West, n.d.).

The Brookings Institution is a nonprofit public policy organization based in Washington, DC. Our mission is to conduct high-quality, independent research and, based on that research, to provide innovative, practical recommendations that advance three broad goals:

- Strengthen American democracy;
- Foster the economic and social welfare, security and opportunity of all Americans;
- Secure a more open, safe, prosperous and cooperative international system.

Brookings is consistently ranked as the most influential, most quoted and most trusted think tank (Brookings Institution, n.d.).

Summary. Darrell West evaluates government agencies that have made the move to cloud computing and discusses the future of cloud computing. Government agencies generally saw between 25 and 50 percent savings in moving to the cloud that translates into billions in cost savings. There is a wide variation of numbers in return on investment since studies demonstrate that savings are not clear across the board ad more case studies are needed.

The type of cloud computing being used affects the potential for costs savings. Factors such as public versus private clouds can make a big difference. An example, for an agency needing 1,000 file server would spend $22.5 million for storage in a public cloud, $28.8 million for a hybrid, and $31.1 million for a private cloud. In addition, the level of privacy and security protection is another key variable migration for government agencies. Some organizations have classified information that requires top levels of security in monitoring and firewalls. The cloud solutions that are provided at the high risk level will cost more because they include secure facilities and personnel with security clearances, and extensive background checks.

The data for this study comes from a series of case studies involving government agencies that have moved to the cloud. For example, in 2009 the city of Los Angeles decided to move e-mail service for 30,000 employees from Novell’s GroupWise onto Google’s cloud services. In a five year cost analysis, the Google cloud would cost $17,556,484 versus the current cost of $22,996.242, which is a 23.6 percent savings for the city of Los Angeles. In another example, data storage for the U.S. Air Force was using 60 file servers but was only utilizing 10 percent of central processing unit capacity. Low utilization levels cost hundreds of thousands of dollars each year. The U.S. Air Force replaced their old file servers with four servers at two sites using an internet cloud to link the data centers.

There are significant varying cost savings with various cloud migrations dependent on the scope of the migrations. Clouds bring conveniences, efficiency, and connect-ability that are vital to government agencies.

Yang, S., Yoo, B., Jahng, J. (2010). Does the saas model really increase customer benefits? *Asia Pacific Journal of Information Systems*. Retrieved from http://apjis.or.kr/pdf/MIS020-002-5.pdf

Abstract. Software as a service (SaaS) is one of the most-talked about trends in IT. Unlike traditional perpetual licensing model, software applications are sold on subscription bases and services are provided over web by the vendors. It is said that SaaS can make vendors to invest more on R&D than on marketing while offering its customers better quality software applications at lower costs. By empirically comparing vendors providing their software applications either by SaaS or by traditional perpetual licensing model, we examine whether or not SaaS really increases overall customer benefits in terms of cost efficiency, software quality, and customization. We show that SaaS may not provide better quality or cost efficient software applications than perpetual licensing does. Then we provide two practical tools, which are useful for customers to evaluate whether SaaS is better than perpetual licensing for the purposes of software applications they want to adopt.

Credibility. Seojung Yang received the BS degree in business administration and Master degree in Management Information Systems (MIS) from the Graduate School of Business at Seoul National University. Seojung's interests are on SaaS, utility computing, virtual organization, and electronic commerce (Yang, Yoo, & Jahng, 2010).

Byungjoon Yoo is an associate professor at the Graduate School of Business at Seoul National University. Byungjoon's research interests are on B2B e-commerce, online auctions and pricing strategies of digital goods such as software products. Byungjoon is published in journals such as Management Science, Journal of Management Information Systems, and Journal of Organizational Computing and Electronic Commerce (Yang, Yoo, & Jahng, 2010).

Jungjoo Jahng is an associate professor of information systems in the College of Business Administration, Seoul National University (SNU). Prior to joining SNU, he was a faculty member of Rensselaer Polytechnic Institute, U.S.A. Jungjoo received his PhD degree in management information systems from the University of Wisconsin, Milwaukee, USA. His research interests are in the domains of electronic commerce IS strategy and IT-based innovation (Yang, Yoo, & Jahng, 2010).

Asia Pacific Journal of Information Systems (APJIS) is published by the Korea Society of Management Information Systems (KMIS), which is the largest professional institute in the field of information systems in Korea. KMIS (http://www.kmis.or.kr) has been publishing the APJIS since the year 1990 and has successfully made it a flagship journal in the information systems field in Korea (APJIS, n.d.).

Summary. This study examines whether or not SaaS really increases customer benefits in terms of cost efficiency, software quality, security, service availability, and customization.

Investment in quality software is one area that cloud providers suggest they accelerate in since they invest in product development. According to figures sampled by the authors, the argument cannot always be supported. In order to provide a study on investment, the authors collected income statements of different groups varying of pure SaaS companies, and those that are hybrids – offer both cloud and in-house solutions. The income statements were used to calculate the proportion of research and development (R&D) in percent of total revenue. From the findings, a hypothesis was formed that no significant difference exists between the mean average percentage of costs spent in R&D of the pure SaaS group and one of the hybrid groups. These are opposite the results from previous studies conducted.

The concept that SaaS is cost efficient and saves on large upfront costs is also contested by the authors. A sample was chosen to compare the net present value of software license fees between two CRM competitors: Siebel and SalesForce. Over a four year period it was calculated that the NPV cost for Siebel's license fee plus annual maintenance fee per user is $2,456. The Sales force subscription fees added up to $2,865 per user. The authors state that the predominant conception of SaaS as cost efficient to customers cannot be supported in all cases.

The total cost of ownership is in using SaaS versus on-premise applications is also important to consider. In traditional on-premise software models, vendors only offer the product and it's up to the customers to maintain and manage the software. If additional support is needed, the traditional vendor will offer it based on a fee. However, in the SaaS model, software vendors provide the software and manage the software on their own servers without additional fees. With SaaS every cost related to software implementation is already included in the subscription fee.

The authors predict that SaaS solutions will become mainstream and more enterprises will adopt them. Some companies will have unique needs and may use SaaS as a supplement to on-premise models depending on the needs of the customers.

The following set of references address potential strengths, weaknesses, opportunities, or threats (SWOT) related to security when using SaaS in support of an EDRMS.

Benlian, A., & Hess, T. (2011). Opportunities and risks of software-as-a-service: Findings from a survey of IT executives. *Decision Support Systems*, *52*(1), 232–246. doi:10.1016/j.dss.2011.07.007

Abstract. IT providers have heralded software-as-a-service (SaaS) as an excellent complement to on-premises software addressing the shortcomings of previous on-demand software solutions such as application service provision (ASP). However, although some practitioners and academics emphasize the opportunities that SaaS offers companies, others already predict its decline due to the considerable risk involved in its deployment. Ours is the first study to analyze the opportunities and risks associated with adopting SaaS as perceived by IT executives at adopter and non-adopter firms. We first developed a research model grounded in an opportunity-risk framework, which is theoretically embedded in the theory of reasoned action. Subsequently, we analyzed the data collected through a survey of 349 IT executives at German companies. Our findings suggest that in respect to both SaaS adopters and non-adopters, security threats are the dominant factor influencing IT executives' overall risk perceptions. On the other hand, cost advantages are the strongest driver affecting IT executives' perceptions of SaaS opportunities. Furthermore, we find significant differences between adopters' and non-adopters' perceptions of specific SaaS risks and opportunities, such as performance and economic risks as well as quality improvements, and access to specialized resources. Our study provides relevant findings to improve companies' assessment of SaaS offerings. It also offers SaaS providers insights into the factors that should be prioritized or avoided when offering SaaS services to companies at different stages of their technology adoption lifecycle.

Credibility. This article was published by Elsevier for the Institute for Information Systems and New Media, University of Munich. Elsevier is a publishing company that publishes medical and scientific literature (Elsevier, 2013).

Alexander Benlian is an assistant professor of the research group "Software & Business" at the Institute for Information Systems and New Media at LMU – Munich School of Management. His undergraduate program was business administration with a focus on information systems and planning/organizations. In 2002, he earned a graduate degree in communication science. Alexander is the author/co-author of more than fifty reviewed articles in journals (Journal of Management Information Systems, Information Systems Journal, European Journal of Information Systems, International Journal of Electronic Commerce, Decision Support Systems, Information & Management Wirtschaftsinformatik/Business & Information Systems Engineering, Wirtschaftsinformatik *& Management*, *HMD*) and conference proceedings (Alexander, n.d.).

Summary. This study analyzes the opportunities and risks associated with using SaaS as perceived by IT executives. Some companies and market researchers are skeptical about SaaS adoption. The main barriers are said to be reliability, security, and privacy concerns. The authors use a perceived risk framework developed by Cunningham in 1967 to provide a hypotheses on risk factors' influence. Perceived risks for SaaS include five factors: performance, economic, strategic, security, and managerial/psychosocial.

Performance risks address the possibility that SaaS won't perform as expected. The SaaS provider may not provide application availability or network bandwidth from the provider may be poor.

Economic risks address the possibility that the client may have to incur unexpected costs to reach the level of service not anticipated.

Strategic risks address the possibility that a company may lose critical capabilities when using applications via SaaS. For example, if business critical applications support key functional areas are on SaaS, there is a high interdependence between the company and the external SaaS provider.

Security risks are possible since the SaaS and the data are hosted on external servers. SaaS clients give a provider control to their data without accurately knowing how the provider secures their data and which backup disaster recovery policies or procedures are in place. Also technology advances so quickly which makes IT environments unpredictable.

Managerial risks may come into existence if perceptions of managers by their peers view outsourcing or using SaaS as a negative for workers.

Breeding, M. (2013). Digital archiving in the age of cloud computing. *Computers in Libraries*, *33*(2), 22–26.

Abstract. The author looks at options provided by cloud computing in protecting and preserving digital assets that represent investments of time and creative energies. He notes that digital storage services provide cloud computing technologies that deliver high levels of protection. The need for proactive attention and planning for responsible care of digital data is discussed as well as the classic approach to disaster recovery planning.

Credibility. Marshal Breeding is the creator of the Library Technology Guides website (www.librarytechnology.org). He writes a monthly column for *Computers in Libraries*, is a contributing editor for *Smart Libraries* newsletter published by ALA Techsource, has written 7 issues of *Library Technology Reports*, and is on the editorial board for Information *Standards Quarterly* published by NISO and Electronic Library (Internet Librarian, 2012).

Information Today, Inc. (ITI) is the publisher of *Information Today,* as well as other periodicals, books, directories, and online products; and is the organizer of Computers in Libraries, Streaming Media, Enterprise Search Summit, and other prestigious conferences and exhibitions for the library, information & knowledge management communities.

Summary. Data created in both the personal and professional world need a reasonable amount of care to protect and preserve digital data that represents investments in time and energy. Cloud computing introduces options to assist in digital preservation that can deliver high levels of protection. Care of digital data requires levels of proactive attention and planning. One should not wait until time of failure to create safeguards. At a minimum there should be a backup and disaster recovery plan in place to protect against equipment failures.

A further challenge is to ensure long term survival of data. Cloud computing opens up a variety of options that can be used for the backup of data. Some vendors offer limited free storage on the cloud such as Dropbox, Microsoft's SkyDrive, and Google drive to name a few.

Most large organizations have enterprise level storage management plans in place that include specific drives in which employees place files that can be backed up with multiple layers of redundancy. This approach supports the development of a disaster recovery plan and should be secured for authorized personnel only. Organizations that maintain enterprise networks make use of industrial strength services that provide features such as encrypted file transfer and storage, private separate cloud storage, data integrity validation, and other processes that are in line with current business practices.

The key to long-term digital preservation involves an institutional commitment to preserve the data with technology platforms that can realistically be expected to exist in the distant future.

Cloud use can complicate e-discovery. (2013). *Information Management Journal*, *47*(1), 17–17.

Abstract. In this article the author discusses how unchecked use of cloud computing can complicate electronic-discovery. Analyst Barry Murphy of the E-Discovery Journal Group believes that organizations must work with cloud service providers (CSPs) on the e-discovery details. The author further informs about the factors mentioned in the book "Outsourcing Records Storage to the Cloud" that should be considered while moving records storage to the cloud.

Credibility. ARMA International is a not-for-profit professional association and the authority on governing information as a strategic asset. The association was established in 1955. Its approximately more than 10,000 members include information managers, information governance professionals, archivists, corporate librarians, imaging specialists, legal professionals, IT managers, consultants, and educators, all of whom work in a wide variety of industries, including government, legal, healthcare, financial services, and petroleum in the United States, Canada, and more than 30 other countries around the globe (ARMA International, n.d.) (b).

ARMA International publishes *Information Management* magazine, the only professional journal specifically for professionals who manage information as part of their job description. The award-winning *IM* magazine is published bi-monthly and features articles on the hottest topics in information governance today, as well as marketplace news and analysis (ARMA International, n.d.) (b).

Summary. Cloud computing use can complicate e-discovery if organizations don't manage their cloud systems well and let them go unchecked. When organizations choose a cloud service provider they should choose one that has an understanding of compliance requirements.

The following factors should be considered when moving records storage to the cloud and should be included in the service level agreement with the cloud provider:

- Create rules for employee's use of corporate information on cloud based systems.
- Ownership of data needs to be established and include language that will protect the organization.

- Establish allocation of liabilities for loss or wrongful disclosure of data within the contract.
- Processes for legal holds should be established and communicated to the cloud provider. It should be made clear in the service contract what the cloud provider's obligations are for implementing and managing legal holds.

Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers & Security*, *29*(2), 196–207. doi:10.1016/j.cose.2009.09.002

Abstract. An organisation's approach to information security should focus on employee behaviour, as the organisation's success or failure effectively depends on the things that its employees do or fail to do. An information security-aware culture will minimise risks to information assets and specifically reduce the risk of employee misbehaviour and harmful interaction with information assets. Organisations require guidance in establishing an information security-aware or implementing an acceptable information security culture. They need to measure and report on the state of information security culture in the organisation. Various approaches exist to address the threats that employee behaviour could pose. However, these approaches do not focus specifically on the interaction between the behaviour of an employee and the culture in an organisation. Organisations therefore have need of a comprehensive framework to cultivate a security-aware culture. The objective of this paper is to propose a framework to cultivate an information security culture within an organisation and to illustrate how to use it. An empirical study is performed to aid in validating the proposed Information Security Culture Framework.

Credibility. *Computers & Security* is the most respected technical journal in the IT security field. Now in its 29th year, the journal is essential reading for IT security professionals around the world. *Computers & Security* provides you with a unique blend of leading edge research and sound practical management advice. It is aimed at the professional involved with computer security, audit, control and data integrity in all sectors - industry, commerce and academia (Computers & Security Journal - Elsevier., n.d.).

Adele de Veiga received her PhD (IT), focusing on information security culture, and the University of Pretora, South Africa. She is a management consultant focusing on information security, risk management and auditing. She is also a Certified Information Systems Auditor (CISA).

Jan Eloff received a PhD (Computer Science) from the Rand Afrikaans University, South Africa. He is head of the department and full time professor in computer science at the Department of Computer Science, University of Pretoria. He has published extensively in a wide spectrum of accredited international subject journals. He is evaluated as a B2 researcher from The National Research Foundation (NRF), South Africa. He is a member of the Council for Natural Scientists of South Africa (Da Veiga & Eloff, 2010).

Summary. The objective of this paper is to propose a framework to create an information security culture within an organization. According to Da Veiga and Eloff (2010), two to three percent of an organization's annual profit may be lost due to information security incidents. Studies show that insiders pose the most threat to the information of an organization. Other research shows that insiders can be behind most of the breaches whether intentional or not. A variety of controls are needed to guard against such breaches and these controls should not just be technical. One measure the authors consider is to develop an *information security aware culture* within the organization. The definition provided by the authors of an information security culture is "the information security perceptions, attitudes and assumptions that are accepted and encouraged in an organization – thus the way in which things are done in an organization to protect information assets" **(**Da Veiga & Eloff, 2010).

The four additional types of culture defined by the authors are:

- Bureaucratic culture – rules of how to protect information assets will be documented and followed.
- Individualistic culture – these organizations one has to involve the individual to obtain their commitment when creating decisions or implementing information security controls.
- Task-based culture – planning control and team responsibilities are important.
- Autocratic culture – leaders are fundamental to implementing any change.

The information security culture framework consists of three main parts: (a) Information security categories, (b) information security behavior, and (c) information security culture. The information security components are implemented in the organization. These components can be seen as the influencers of the information security behavior in the organization. In time, this security behavior evolves as the way things are done around the organization.

The objective is to instill information security that conduces the protection of information assets based on the information security policies. The framework provides a guidance to engage an information security culture that produced acceptable behavior towards security.

Devereaux, R. L., & Gottlieb, M. C. (2012). Record keeping in the cloud: Ethical considerations. *Professional Psychology: Research and Practice, 43*(6), 627–632. doi:10.1037/a0028268

Abstract. Innovations in the production, storage, protection, and retrieval of digital information occur at breakneck speed. With them can come perceived pressure to transition from paper to electronic records, because doing so may appear to offer benefits for improved patient care. At the forefront of this shift is the popularization of "cloud" computing. While "the cloud" has entered our everyday parlance from Internet-connected televisions to smart phones that track and control our finances, little has been written about how this technology functions and how it may expose practitioners to unforeseen and previously nonexistent risk. In this article we define "the cloud," discuss risks and benefits of its use, and provide questions for practitioners to ask when considering the appropriateness of maintaining patient records in this manner. Considerations are made in light of current federal legislation and recommendations, professional ethical standards and guidelines established by the American Psychological Association, and ethical decision-making practices.

Credibility. The American Psychological Association is the largest scientific and professional organization representing psychology in the United States. APA is the world's largest association of psychologists, with more than 134,000 researchers, educators, clinicians, consultants and students as its members. The mission is to advance the creation, communication and application of psychological knowledge to benefit society and improve people's lives (APA, n.d.).

Summary. Record keeping in the cloud is analyzed in this paper in accordance with the American Psychological Association (APA) record keeping guideline. An example of an APA standard is standard 4.01, which refers to maintaining confidentiality. Standard 4.01 has a primary obligation to take reasonable steps to protect confidential information obtained through or stored in any capacity.

As records move to the cloud, the ability to keep confidentiality may diminish to an unknown degree. Furthermore, when the aggregation of sensitive data is stored large data centers it can increase the appeal for potential cybercriminals to attempt to steal the information.

An issue with regards to confidentiality is the potential risk to privacy. When technical difficulties arise once documents are stored in the cloud, a practitioner may be required to expose or discuss patient records to a technical person in order to provide support and fix the problem. In a large hospital setting, technical employees are monitored in their work when they are exposed to patient data. In a cloud environment it cannot be guaranteed that their technical people will be monitored because they may be unfamiliar with such compliance obligations.

Further issues arise can arise when trying to port over to a different cloud vendor. One example can be trying to change service providers, only to encounter the inability (or difficulty) to transfer data because the system that was currently being used is proprietary. This can cause longer than expected down times and patient records may not be accessible.

The APA has recommendations for the issues they have outlined:

- Understand what record keeping guidelines are needed for the clinical environment. One example is to store non-sensitive records in the cloud.
- Question the cloud service provide on how the manage external and internal security.
- Consult with insurance and legal parties to understand covered protection if a breach of security were to occur.
- Use established cloud storage firms.
- Use the cloud for the purpose of backup only and keep a second set of records in a different location.
- Read and understand the terms of use, privacy policy and other service agreements completely.
- Consider developing a two-tiered identification system. This will enhance security as records of patients will be split in two separate locations.

Practitioners moving to the cloud should do so with caution and careful consideration of the risks and benefits.

Farrell, R. (2010). Securing the cloud-governance, risk, and compliance issues reign supreme. *Information Security Journal: A Global Perspective*, *19*(6), 310–319.

Abstract. While acknowledging the many benefits that cloud computing solutions bring to the world, it is important to note that recent research and studies of these technologies have identified a myriad of potential governance, risk, and compliance (GRC) issues. While industry clearly acknowledges their existence, timing-wise it is still well before the legal framework has been put in place to adequately protect and adequately respond to these new and differing global challenges. This paper seeks to inform the potential cloud adopter, not only of the perceived great technological benefit, but to also bring to light the potential security, privacy, and related GRC issues which will need to be prioritized, managed, and mitigated before full implementation occurs.

Credibility. Taylor & Francis Group is an international company originating in the United Kingdom that publishes books and academic journals. It is a division of Informa plc, a United Kingdom-based publisher and conference company (Taylor & Francis, 2013).

Rhonda Farrell is a current Doctoral student at the University of Fairfax and is an Associate at Booz Allen Hamilton. Rhonda has worked in Silicon Valley, CA, within the operations, engineering, quality, and security portions of major firms, such as Cisco Systems, Inc. and VISA, among others. She graduated in 2009 from Concord Law School with her JD and in 2010 relocated to the East Coast to continue her career, focusing on the cyber-security realm **(**Farrell, 2010).

Summary. There are many security breaches that are documented for on premises solutions. For example, the Ponemon Institute found that more than 250 million records containing confidential or sensitive data have been breached since 2005 with the total monetary value per breached record to be $202 in 2008. The same study also reported internal security breaches that were either negligent or malicious. Lack of resources or budgets where contributing factors to the security breaches.

Cloud computing can fill the resources or budget voids by implementing a cloud based solution. Before implementing the cloud, there are possible security issues a cloud solution can also have and the author lists possible mitigations that should occur before implementation. The Open Web Application Security Project (OWASP) released a cloud top 10 security risks that includes:

1) Accountability (SLA, data ownership, security, jurisdictional constraints.)
2) Federated identity management
3) Regulatory compliance
4) Business continuity
5) User privacy and secondary usage of data
6) Service and data integration
7) Multi-tenancy and physical security
8) Incidence analysis and forensic support
9) Infrastructure security
10) Non-production environment exposure (testing sites)

The above risks are currently being addressed by a wide selection of cloud technology providers in order to achieve the security objectives of organizations. It's recommended that enterprises going onto the cloud create a checklist which identifies risks associated with "contracts/SLA's (services, record management and compliance obligations, security controls, data destruction, minimum and maximum retention periods per data classification level, secure destruction options, backups, replication, failover, assurance of disposition within agreements), audit controls (audit processes, standards adherence, compliance auditing), integration (interoperability, compliance tools), policies and procedures (acceptable records management mechanisms in place), and data (data mapping to show where data resides)" (Farrell, 2010).

Ferguson-Boucher, K., & Convery, N. (2011). Storing information in the cloud – a research project. *Journal of the Society of Archivists*, *32*(2), 221–239. doi:10.1080/00379816.2011.619693

Abstract. Cloud computing as a new delivery model is proving challenging for recordkeeping professionals. The ARA/Aberystwyth University research project, 'Storing Information in the Cloud' aimed to investigate the management, operational and technical issues surrounding the storage of information in the cloud. It also set out to develop a toolkit that could assist information professionals in assessing the risks and benefits of outsourcing information storage and processing. Based on the information gathered through a literature review, questionnaire, an unconference, as well as interviews with cloud providers and customers, the outcomes included the Cloud Computing Toolkit, a list of cloud computer resources relevant to the records and information community and specific recommendations. These include further research into the implications of cloud computing for record-keeping principles and practice and the development of cloud-specific guidance and policies and a pool of resources relating to cloud computing and information management. The extension of the research to consider its implication for the long-term preservation of digital material was also a recommendation and the development of a more active role for professional bodies in bringing together information professionals and in forming interest/working groups on specific related to cloud computing. New technologies or new models continue to challenge the profession's ability to maintain information governance and assurance and on-going research is required to ensure that we address the practical and strategic issues of the fluid information ecology.

Credibility. Kirsten Ferguson-Boucher is a lecturer at the Aberystwyth University in the United Kingdom. Kirsten's undergraduate teaching includes records management in an electronic age, and her postgraduate teaching includes records management in an electronic age, records management, digital records, records and information governance. Kirsten has been published in the *Journal of the Society of Archivists, Public Sector Records and Information Management Conference, Cloud Futures Workshop 2011 with Microsoft Research, University of British Columbia,* and many other publications (Aberystwyth University, n.d.).

Nicole Convery is the other author of this literature. Nicole was a teaching fellow for the Aberystwyth University in the United Kingdom between October 2008 and February 2011. Nicole's publications were published in *The Future of Archives and Recordkeeping, Archives and Records Association,* and the *Archives and Records Association* (Convery, n.d).

Summary. Ferguson-Boucher and Convery (2011), provide studies of information management aspects of cloud computing in this literature review. This study suggests that cloud computing is invading the corporate environment. Cloud computing is described as the ability to access a network of computing resources which are owned and maintained by a third party via an internet connection. The cloud is composed of hardware, storage, networks, and services that are accessed by an end user on demand at any location. A survey from thirty participants with information management professional backgrounds show concerns ranging from security to data integrity and are discussed in detail. The main concerns of the participants included (in order of importance):

- Retrieval and/or destruction of data when service terminated.

- Loss of control over data and services
- Data protection
- Confidentiality of data/unauthorized access
- Availability and reliability of services
- Integrity of data
- Ability to audit service
- Compliance and e-discover
- Infrastructure and network security
- Lack of customization/integration with existing systems
- Portability and interoperability of cloud services
- Unknown cost due to variable pricing structure

Organization's main drivers for cloud computing are (in order of importance):

- Reduced IT spending
- High flexibility and scalability
- Optimization of IT infrastructure
- Access to applications not available in-house
- Business continuity and disaster recovery
- Improved reliability
- Ease of use
- Modernization of business processes

Kamal, S., & Kaur, R. (2011). Cloud computing security issue: Survey. *AIP Conference Proceedings*, *1414*(1), 149–153. doi:10.1063/1.3669947

Abstract. Cloud computing is the growing field in IT industry since 2007 proposed by IBM. Another company like Google, Amazon, and Microsoft provides further products to cloud computing. The cloud computing is the internet based computing that shares resources and information on demand. It provides the services like SaaS, IaaS and PaaS. The services and resources are shared by virtualization that run multiple operation applications on cloud computing. This discussion gives the survey on the challenges on security issues during cloud computing and describes some standards and protocols that presents how security can be managed.

Credibility. *AIP Conference Proceedings* is a series of scientific journals published by the *American Institute of Physics* since 1970. The journal publishes the proceedings from various meetings of physics societies. *AIP Conference Proceedings* publishes more than 100 volumes per year, with back-file coverage to 1970, which encompasses 1,330 proceedings volumes and 100,000 published papers **(**AIP Conference Proceedings, 2013)**.**

Summary. This paper outlines potential types of attacks when using cloud computing and provides standards and protocols that present how security can be managed. The three types of attacks against cloud computing addressed in this paper are:

- Cloud malware injection attack – creates its own malicious service implementation (i.e. SaaS) and adds it to the cloud system.
- Flooding attacks – consists of an attacker sending large amounts of non-relevant requests to the cloud service provider.
- Metadata spoofing attack – aims at maliciously reengineering web services metadata descriptions.

A method that can provide adequate levels of protection is known as *identity and access management* (IAM). IAM protects an organization through rules and policies which are enforced on users via techniques such as (a) authentication, (b) authorization, and (c) auditing.

Two main protocols for security to the cloud considered by IAM are (a) security assertion markup language (SAML) and (b) open authentication protocol (OAuth). SAML is based on XML standards and is used as a tool to exchange authorization and authentication between two entities. OAuth allows users to share their private data on one cloud service provider with another cloud service provider without exposing sensitive personal information like user names and passwords.

Cloud service providers may prefer more than one authentication protocol to provide better security. The SAML is mostly used at the enterprise level due to its single sign on (SSO) functionality. Data encryption keys and auditing of the system are the main requirements for cloud computing.

Kaufman, L. M. (2009). Data security in the world of cloud computing. *IEEE Security Privacy*, *7*(4), 61–64. doi:10.1109/MSP.2009.87

Abstract. Today, we have the ability to utilize scalable, distributed computing environments within the confines of the Internet, a practice known as cloud computing. In this new world of computing, users are universally required to accept the underlying premise of trust. Within the cloud computing world, the virtual environment lets user's access computing power that exceeds that available within their physical worlds. Typically, users will know neither the exact location of their data nor the other sources of the data collectively stored with theirs. The data you can find in a cloud ranges from public source, which has minimal security concerns, to private data containing highly sensitive information (such as social security numbers, medical records, or shipping manifests for hazardous material). Does using a cloud environment alleviate the business entities of their responsibility to ensure that proper security measures are in place for both their data and applications, or do they share joint responsibility with service providers? The answers to this and other questions lie within the realm of yet-to-be-written law. As with most technological advances, regulators are typically in a "catch-up" mode to identify policy, governance, and law. Cloud computing presents an extension of problems heretofore experienced with the Internet. To ensure that such decisions are informed and appropriate for the cloud computing environment, the industry itself should establish coherent and effective policy and governance to identify and implement proper security methods.

Credibility. The primary objective of *IEEE Security & Privacy* is to stimulate and track advances in security, privacy, and dependability and present these advances in a form that can be useful to a broad cross-section of the professional community--ranging from academic researchers to industry practitioners. *IEEE Security & Privacy* aims to provide a unique combination of research articles, case studies, tutorials, and regular departments covering diverse aspects of security and dependability of computer-based systems **(**IEEE Security and Privacy, n.d.).

Lori M. Kaufman is a deputy chief technology officer at BAE Systems. Her research interests include cyber security, software assurance, and biometrics. Kaufman has a PhD in electrical engineering from the University of Virginia (Kaufman, 2009).

Summary. This article highlights questions that are yet to be fully answered from a cloud security perspective. For example, is security solely the storage provider's responsibility, or is also the responsibility of the organization that leases the applications? The data found in a cloud ranges from public source, which has minimal security concerns, to private data containing highly sensitive information (such as social security numbers, medical records, or shipping manifests for hazardous material).

To ensure data confidentiality, integrity, and availability (CIA), the cloud provider must offer minimum capabilities that include:

- A tested encryption storage that ensures the shared storage safeguards all data;
- Stringent access controls to prevent unauthorized access
- Scheduled data backup processes and provide safe storage to the backup media.

To overcome security concerns and undefined roles on who is ultimately is responsible for security, the adopters of cloud computing must develop a security model that promotes CIA. Cloud providers could enable this type of CIA model, but the difficulty is obtaining security data from providers. This problem has existed ever since computers have been used to secure data for financial companies, businesses, and national security concerns.

To advance cloud computing, the cloud community must take proactive measures to ensure security. A movement exists to adopt universal standards, such as open source, to ensure interoperability amongst cloud providers. Included in this movement is to develop a security standard that ensures CIA. Legal decisions will ultimately determine who owns the responsibility for securing information shared within the cloud environment.

To assist in future decisions that will enhance the cloud-computing environment, the industry itself should establish effective policies and governance. The US National Institute of Standards and Technology (NIST) has created a cloud computing security group to assist in policy creation. NIST envisions its role as “the effective and secure use of the technology within government and industry by providing technical guidance and promoting standards” Kaufman, 2009).

Sehgal, N. K., Sohoni, S., Ying Xiong, Fritz, D., Mulia, W., & Acken, J. M. (2011). A cross section of the issues and research activities related to both information security and cloud computing. *IETE Technical Review*, *28*(4), 279–291. doi:10.4103/0256-4602.83549

Abstract. Cloud computing amplifies computer security issues that have proliferated with the growth of the Internet. A broad range of security research is being applied to cloud computing. This paper gives a description of cloud computing followed by a general description of information security issues and solutions, and a brief description of issues linking cloud computing with information security. Security solutions must make a trade-off between the amount of security and its performance cost and impact on the end-user experiences. This is accentuated in a cloud computing environment where users desiring different levels of security share the same resources. An essential issue for cloud computing is the perception of security, which is beyond the simple technical details of security solutions. This paper includes a list of a few key information security challenges that also present significant research opportunities. Solving these key problems will encourage the widespread adoption of cloud computing.

Credibility. The IETE is the National Apex Professional body of Electronics and Telecommunication, Computer and IT Professionals, focusing on advancements in science and technology. Towards this end, the Institution promotes professional development and conducts basic engineering and continuing technical education programs for human resource development. Today, it has more than 69,000 members, individuals and industries / organizations through its 55 regional centers spread all over India including one in Kathmandu. The IETE is recognized as a Scientific and Industrial Research Organization (SIRO) by Dept. of Science & Industrial Research, Ministry of Science and Technology, Government of India. Its activities span from education to technology and research & development (IETE Technical Review, n.d.).

Dr. Naresh Sehgal holds a PhD in computer engineering from Syracuse University and an MBA from Santa Clara University. He holds 4 patents and has authored more than 20 publications.

Dr. Sohum Sohoni is an Assistant Professor in the School of Electrical and Computer Engineering at Oklahoma State University. He has a PhD in computer engineering from the University of Cincinnati. Dr. Sohoni's research interests are broadly in the area of computer architecture and performance analysis.

Ying Xiong holds a MS degree in electrical engineering from Wuhan University of Technology. His research interests include secure processor and its co-design with secure operating system.

David Fritz is a Doctoral Candidate in Electrical and Computer Engineering at Oklahoma State University. His research interests are in Computer Engineering Education and Computer Architecture.

Wira Mulia is a Doctoral Candidate in Electrical and Computer Engineering at Oklahoma State University. His research interests are in Computer Architecture and Systems.

Dr. John M. Acken has been at OSU-Tulsa since 2001. Acken received his BS and MS in Electrical Engineering from Oklahoma State University and his PhD in Electrical Engineering from Stanford University. At OSU-Tulsa, Dr. Acken's projects include technology and devices for information security and identity authentication.

Summary. This paper provides a general description of information security issues and potential solutions linking cloud computing with information security. Information security is defined as the protection of data and processing from unauthorized observation, modification, or interference. Cloud computing requires a holistic security approach to cloud security.

Information security includes three functions:

- Access control – this includes the initial entrance by a participant and the reentry of the participant.
- Secure communications – includes any transfer of information among participants.
- Protection of private data – includes storage devices and processing units.

The traditional approach to information security relied upon physical barriers. For example the computing center access is only available to key personnel, or system administrators who have special access lines.

The internet introduces many possible obstacles in security. When using an open channel or the internet, it provides intruders with unlimited tries to gain access to systems for which they are not authorized. Hackers find ways to spoof IP addresses and failed attempts for log-ins cannot be traced. The security of cloud computing varies with the model used (SaaS, PaaS, or IaaS), but the most frequently analyzed model is the public cloud model (Saas).

Some key challenges to the public cloud model include:

- Privacy – Cloud users may not know where their data is being storage or processed.
- Boundaries – Clear security walls are not apparent as the cloud used distribution methods to share and spread information.
- Trust – Information stored on cloud services are at risk of attackers.
- Data integrity – Data from potentially competing sources could reside on the same structure, and through by accident a computer process can violate the virtual boundary.

Shute, W. (2012). Information governance takes center stage in 2013: Spotlight shines on IG pros. *Information Management Journal, 46*(6), 22–25.

Abstract. The article focuses on the heightened information governance in 2013 that would provide opportunity for information governance professionals in the U.S. It mentions that 1.8 trillion gigabytes of electronic information were produced only in 2011, which lead to greater electronic information in the future, according to the study conducted by IDC. It states that information technology (IT) leader should implement comprehensive information governance programs, including inventory, organize and control, to cope with the increasing changes of volumes. It says that cloud-based tools for sharing of files and collaboration are in growing use in 2012.

Credibility. ARMA International publishes *Information Management* magazine, the only professional journal specifically for professionals who manage information as part of their job description. The award-winning *IM* magazine is published bi-monthly and features articles on the hottest topics in information governance today, as well as marketplace news and analysis (ARMA International, n.d.)

Summary. Organizations have vast amount of growing data and expanding varieties that may include audio, video, documents, e-mail, and social media. A 2011 Digital Universe study finds that businesses would create and replicate more than 1.8 trillion gigabytes of electronic information in 2011. As company data grows into the terabytes, petabytes, and exabytes, the records manager will find more opportunities to work with IT on technology selection and cloud initiatives. Furthermore, the records manager function will continue to evolve and may catapult the records management responsibility into the spotlight for businesses looking to protect their data. These challenges will drive the five leading predicted data management trends to emerge in 2013**:**

- Records Management will move to the forefront – Protecting and managing exclusive data via information governance best practices and technology will gain greater importance. These efforts will require records managers to continue educating themselves on what drives IT and the business and can leverage their knowledge with information governance to accomplish corporate goals.
- Organizations will implement needed change and improvements – Businesses have realized they can no longer put off information governance programs in order to inventory organize, control and understand what data is stored throughout the organization.

- Information Governance will become a cost-reduction driver – Records management will focus on reducing cost and risk through the organization.
- The cloud will receive greater scrutiny and security – Organizations are experiencing growing use of mobile and cloud technologies for file sharing. Organizations see threats of these technologies if they go ungoverned. In 2013, organizations will increase their use of private or hybrid clouds to meet their mobile workforce needs.
- Consolidation, content analytics, and streamline e-discovery – The cloud archiving market is changing the landscape for e-discovery and information management. There will be fewer providers but the providers will be focused on delivering strategic products.

Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security, 29*(4), 476–486. doi:10.1016/j.cose.2009.10.005

Abstract. Information technology has become an integral part of modern life. Today, the use of information permeates every aspect of both business and private lives. Most organizations need information systems to survive and prosper and thus need to be serious about protecting their information assets. Many of the processes needed to protect these information assets are, to a large extent, dependent on human cooperated behavior. Employees, whether intentionally or through negligence, often due to a lack of knowledge, are the *greatest threat* to information security. It has become widely accepted that the establishment of an organizational sub-culture of information security is *key* to managing the human factors involved in information security. This paper briefly examines the *generic* concept of corporate culture and then borrows from the management and economical sciences to present a conceptual model of information security culture. The presented model incorporates the concept of *elasticity* from the economical sciences in order to show how various variables in an information security culture influence each other. The purpose of the presented model is to facilitate conceptual thinking and argumentation about information security culture.

Credibility. *Computers & Security* is the most respected technical journal in the IT security field. Now in its 29th year, the journal is essential reading for IT security professionals around the world. *Computers & Security* provides a unique blend of leading edge research and sound practical management advice. It is aimed at the professional involved with computer security, audit, control and data integrity in all sectors - industry, commerce and academia (Computers & Security Journal - Elsevier., n.d.).

Johan van Niekerk is a senior lecturer in the Department of Information Systems at the Nelson Mandela Metropolitan University. He has been in the employment of the NMMU for the past 13 years and has been a full-time academic for the past 9 years. He is currently working towards a PhD as part of the research efforts at the Institute for Information and Communication Technology Advancement. His research focuses on the human factors in information security (Van Niekerk, & Von Solms, 2010).

Professor Rossouw von Solms is a well-known researcher in information security. He has had many previous publications in this field and is employed as a full-time researcher in the Institute for Information and Communication Technology Advancement at the Nelson Mandela Metropolitan University (Van Niekerk, & Von Solms, 2010).

Summary. This paper briefly describes the generic concept of corporate culture and presents a conceptual model of an information security culture.

Many organizations will be unable to proceed with business if they lose access to their information resources. Protecting these resources often have no direct return on investment, therefore business people are rarely interested in how their information resources are protected. According to Niekerk and Von Solms, 2010, it can be argued that the goal of securing information is in conflict with business goals of maximizing productivity and reducing cost.

Information security consists of many processes in which some are dependent on human behavior. Employees are the greatest threat to information security either due to intention, lack of knowledge, or negligence. For this issue, many studies have shown that the establishment of an information security culture in an organization is necessary for effective information security.

Corporate culture exists on different levels:

- Level 1 - Artifacts – What can be seen, heard, and felt in an organization (i.e. visible organizational structures and processes).
- Level 2 – Espoused values – The reasons an employee would give for the observed artifact (i.e. documents that describe the company values).
- Level 3 – Shared tacit assumptions – Implied assumptions usually from beliefs and values that continue to be successful or from the company's early years.

A fourth level, information security knowledge can be added to the model for corporate culture. In an information security culture there is a casual relationship between the artifact, espoused values, shared tacit assumptions, and information security knowledge. For example the visible artifacts, is caused by the effects of the espoused values, shared tacit assumptions, and the information security knowledge. The authors introduce demand and elasticity in presenting the employees in adhering to security procedures or not wanting to adhere to the procedures (elasticity) based on management security higher values (demand).

The model created shows that management demands and employee participation are interrelated. In any information security culture a certain form of elasticity will be present. This elasticity will determine whether the tacit assumptions will over time align to the espoused values of the organization. With education aimed at improving employee attitudes towards information security, organizations can reduce the elasticity in the culture and speed up the pace at which measureable artifacts become more in line with the espoused values.

Conclusion

The purpose of this annotated bibliography is to assist Records and Information Management (RIM) professionals tasked with creating an electronic document and records management system (EDRMS) in the cloud. This scholarly annotated bibliography presents and summarizes 30 references, including peer-reviewed articles, journals, independent research, books, and news media. References examine four main themes of using software as a service (SaaS) in support for an electronic document and records management systems (EDRMS): (a) SaaS definition; (b) EDRMS definition; (c) a SWOT analysis concerning *cost*, related to use of SaaS in support of an EDRMS; (d) a SWOT analysis concerning information *security*, relate to use of SaaS in support of an EDRMS.

SaaS Defined

SaaS is one of three main service models of cloud computing (SaaS, PaaS, and IaaS) (Mell & Grance, 2011). Gartner (n.d.) (b) defines SaaS as "software that is owned delivered and managed remotely by one or more providers. The provider delivers software based on one set of common code and data definitions that is consumed in a one-to-many model by all contracted customers at any time on a pay-for-use basis or as a subscription based on use metrics" (para. 1). The National Institute of Standards and Technology (NIST) define cloud computing as "cloud computing is a model for enabling ubiquitous convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models" (Mell & Grance, 2011, p.2).

According to Orlando (2011), SaaS represents the potential for a low-cost strategy for businesses to use software on demand rather than buying a license for every computer. Statistics from an InformationWeek Analytics 2010 Outsourcing survey show that out of 530 respondents, 68% use some form of SaaS and 37% suggest that SaaS provides higher-quality results at a lower cost (Healey, 2010).

SaaS (cloud computing) have five essential characteristics as listed by Barnes, 2010:

- On-demand self-service – A company can automatically request computing capabilities to increases as needed without requiring human involvement from the service provider.
- Broad network access – Cloud services can be accessed over networks via standard options via a thin or thick client (i.e. mobile phones, laptops, and PDAs) as well as other traditional or cloud-based software services.
- Resource pooling - Used by third-party providers in order to serve multiple organizations utilizing a multi-tenant mode. Each organization has different physical and virtual resources which are assigned or re-assigned according to organizational demand.
- Rapid elasticity - Allows capabilities to automatically scale up or down to meet organizational needs.
- Measured service - Cloud providers automatically control and optimize resources usage through monitoring, controlling and reporting to the organizations.

Choosing a SaaS deployment model is important and should be considered by RIM practitioners in conjunction with the IT department in determining a cloud based deployment model for a RIM system (Barnes, 2010). According to Barnes (2010), the four possible deployment models are:

- Public cloud – The cloud infrastructure is made available to the general public or large industry groups. It is owned by the cloud provider.
- Private cloud – The cloud infrastructure is operated for a single organization. The location of the infrastructure can be on or off premise. If the infrastructure is on premise, then it is managed by the organization. Conversely, if the infrastructure is off premise, then it is managed by a third party.
- Community cloud – The cloud infrastructure is shared by several organizations and supports a shared concern (i.e., mission, security requirement, policy, or compliance).
- Hybrid cloud – The cloud infrastructure is made up of two or more clouds (private, community, or public). This setup is unique and is bound together by standardized, proprietary technology.

Not all so called SaaS providers are the same (Tolliver-Nigro, 2009). Understanding the architecture of a SaaS provider will enable the organization to differentiate between an application service provider (ASP) and a SaaS provider (Tolliver-Nigro, 2009). ASP focuses providing software services on one main server. If the server reaches critical mass, the clients are transferred to another server that can support the increase in use. A true SaaS offering is multi-tenant. With multi-tenant, the SaaS vendor runs the product on a single instance, on multiple machines using a single data set source. The architecture supports a single data set source and code and provides application programming interfaces (APIs). In addition, if these servers reach their bandwidth max, other servers turn on and support the service in the same way automatically

(Tolliver-Nigro, 2009). When virtualization is used in Saas to hide the physical characteristics of a computing platform, the emulated computing platform acts like an independent system that can be configured on demand and maintained easily (Marston, Li, Bandyopadhyay, Zhang, & Ghalsasi, 2011).

EDRMS Defined

An EDRMS combines document management and records management functionality. EDRMS can bring the following benefits to an organization (State Records NSW, n.d.):

- Facilitate the move from paper to digital records
- Improve business efficiency and productivity
- Security of documents
- Provide accountability and transparency for compliance
- Enable to provide recordkeeping at a large scale.

According to ISO 15489-1, records management (RM) is defined as "the field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including the processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records" (Alalwan, & Thomas, 2011).

When considering moving to an EDRMS, an assessment should be made to take into consideration the company's information architecture, current business systems, recordkeeping culture, review policies and procedures, and understand the existence and current use of information and recordkeeping tools. According to Shute (2012), records management will move to the forefront by protecting and managing exclusive data via information governance best practices and technology. These efforts will require records managers to continue educating themselves on what drives IT and the business and can leverage their knowledge with information governance to accomplish corporate goals.

A strategically aligned plan is needed for RIM goals when introducing new technology (Empel, 2012). The different strategies outlined are:

- Systems strategy – This strategy provides a plan and detail on how specific technologies fit into the organization.
- Acquisition strategy – Acquisition decisions should be based on business needs, recordkeeping capabilities, and whether the new technology can evolve with the business.
- Technical strategy – Technical requirements vary on a case-by-case basis, but some considerations include hardware, software, platform, connectivity, administration, support, and maintenance.

Factors To Consider On The Cost of SaaS

Strengths. Cloud based solutions offer ease of management since the cloud provider assumes management related responsibilities, upgrades, and maintenance of hardware and software (Tak, Urgaonkar, & Sivasubramaniam, 2013). A survey conducted by Gartner Research indicates that about two-thirds of corporate IT budgets go towards routine support and maintenance (Marston, Li, Bandyopadhyay, Zhang, & Ghalsasi, 2011).

Cloud use also offers capital expenditure savings and operation expenditure savings by eliminated the need to purchase infrastructure and elimination of additional staffing related costs (Tak, Urgaonkar, & Sivasubramaniam, 2013). Cloud computing can lower IT barriers to innovation. An example of companies that use the cloud for their businesses are startups such as Facebook, YouTube, TripIt, and Mint (Marston, Li, Bandyopadhyay, Zhang, & Ghalsasi, 2011).

SaaS is gaining popularity among organizations (McAffe, 2012). The state of Oregon has partnered with Autonomy to use HPTRIM for a cloud-based SaaS records management system that will allow state, city and county agencies to securely manage and provide access to their digital and physical documents. The cloud-based system is called Oregon Records Management Solution (ORMS) and will be a first of its kind to run statewide. Before using HP TRIM, Oregon employees had to work through back-up tapes, e-mails, and file servers to satisfy requests from the public. With HP TRIM, such requests now take only a matter of seconds to fulfill. For example, a request for 80,000 e-mails generated by the Secretary of State since taking office, took 90 seconds to complete instead of taking days. Because ORMS is cloud-based, there are no up-front infrastructure costs and much lower costs on equipment, power and facilities expenses (Thomson Reuters, n.d.).

Weaknesses. Not all cloud use will have the same savings for everyone, and some may not even offer savings in the end (Tak, Urgaonkar, & Sivasubramaniam, 2013). The type of cloud service used affects the potential for costs savings. Factors such as public versus private clouds can make a big difference. As an example, an agency needing to handle 1,000 file servers would spend $22.5 million for storage in a public cloud, $28.8 million for a hybrid, and $31.1 million for a private cloud (West, 2010).

Some research suggests that SaaS saving are not supported in all cases (Yang, Yoo, & Jahng, 2010). A research study compares the net present value (NPV) of software licenses fees between two CRM competitors: Siebel and SalesForce. This study shows that over a four year period the NPV cost for Siebel's license fee plus annual maintenance fee per user is $2,456. The SalesForce subscription fees added up to $2,865 per user (Yang, Yoo, & Jahng, 2010). In addition, further economic risks address the possibility that the client may have to incur unexpected costs to reach the level of service not anticipated (Benlian & Hess, 2011).

Cloud organizations do not usually provide a suite of applications that an organization can use. Most cloud solutions focus on a specific module. This multivendor environment can lead to additional costs like integrations, end user support, upgrade management, testing and workflow (Herbert & Erickson, 2011). Cloud applications require focus on contracting, managing, service level agreements (SLA's), and performance management. Contract dates can vary widely and would require the organization employing SaaS to constantly monitor and manage vendors (Herbert & Erickson, 2011).

Opportunity. Small business represents a huge opportunity for cloud computing because small businesses can now use high-end applications that were only available to bigger rivals (Marston, Li, Bandyopadhyay, Zhang, & Ghalsasi, 2011).

Another opportunity is the potential to help developing countries benefit from information technology without requiring large up front infrastructure investments that have slowed down past efforts (Marston, Li, Bandyopadhyay, Zhang, & Ghalsasi, 2011). According to Marston, Li, Bandyopadhyay, Zhang, & Ghalsasi (2011), "cloud computing might do to computing in developing countries what mobile phones did to communications – allow the government and local firms to benefit from the effective use of information technology" (p. 181).

Cloud-computing can also help in reducing an organization's carbon footprint. According to a Forrester survey, 41% of people in IT departments believe energy efficiency and recycling are important factors to consider. Implementing green IT, 65% of people from the survey believe that reducing the energy related consumption will saving in operating costs (Marston, Li, Bandyopadhyay, Zhang, & Ghalsasi, 2011).

Threats. Some cloud companies may use proprietary systems that can lock in their customers and can gradually cost more over time. To combat this proprietary systems issue, the international Organization for Standardization (ISO) technical committee for IT has formed a new sub-committee with the goal of collaborating with appropriate bodies. This collaboration can bring the development of interoperable application platforms and service standards in relevant areas (Marston, Li, Bandyopadhyay, Zhang, & Ghalsasi, 2011).

Hidden costs can mostly be avoided if an organization understands their planned usage as best as possible from the beginning. Some cloud contracts won't include items such as mobile access, or test environments. Knowing these needs from the beginning will help with negotiations (Herbert & Erickson, 2011). There are often cases where companies have large volumes of data that need to be used with the SaaS application. It is important to work with the SaaS provider early in the process to understand potential ramifications. Understanding current data sizes and future growth will help an organization understand their data storage limits and avoid incurring additional costs.

Other potential threats include: (a) when IT departments view cloud computing as a threat to their jobs, and (b) concerns about the cloud provider going into bankruptcy (Marston, Li, Bandyopadhyay, Zhang, & Ghalsasi, 2011).

Factors To Consider On The Security of SaaS

Strengths. In a SaaS model, the cloud provider supplies the facilities, infrastructure, hosted applications, and environment in order for personnel to use the cloud software via a web browser. The cloud provider has the responsibility to provide a cloud solution that is required by the customer (organization) via a contract and service level agreements that specifically include:

security controls and technologies at all layers, related governance, compliance related solutions, and possibly having sole responsibility if ever a breach were to occur (Farrell, 2010).

A study conducted in 2009 by the Ponemon Institute titled "U.S. Cost of Data Breach Report" highlights that more than 250 million records containing confidential or sensitive data have been breached since 2005, with a total cost per breached record estimated to be $202 in 2008 (Farrell, 2010). This same study showed that internal security related incidents accounted for 56% versus 44% for third party incidents. Respondents to the study reported lack of resources to combat security related issues as a top challenge (Farrell, 2010).

Security risks can generally be transferred to the service provider within the service level agreement. Security risks can also be mitigated through audit and monitoring of the provider's services and infrastructure. Third-party cloud services that specialize in offering value added services such as Cloudreach can provide these monitoring services (Ferguson-Boucher & Convery, 2011). According to Ferguson-Boucher & Convery (2011), a risk framework to approach cloud as a storage solution for RIM are divided into three categories: preparing, managing, and operating in the cloud.

Preparing for cloud use should focus on alignment with business objectives such as:

- The legal framework in which organizations operate;
- The existing internal systems for staff and other resources;
- The IT infrastructure;
- Central business drivers and current initiatives.

Managing the cloud consists of ensuring the information stored on the cloud continues to be of use to the organization. A guarantee relating to the continuing authenticity, reliability and integrity of the information is required and can be dictated by legal and regulatory compliance.

All considerations with managing information in the cloud are best approached using a risk framework. An organization can determine if the mitigation strategy for the risk is sufficient to address identified issues. Continually reassessing and applying risk criteria a balanced approach to cloud usage is achievable (Ferguson-Boucher, & Convery, 2011).

Operating in the cloud continues to rely on RIM and IT professionals to access policies and procedures for physical, personnel, infrastructure, information and access security. The availability of the service is crucial, as are adequate service levels and ensuring the benefits stated by the cloud provider such as rapid scaling are achievable (Ferguson-Boucher, & Convery, 2011).

SaaS adoption will assist organizations in refocusing on their core competencies. This refocusing will be possible by transferring the responsibility of developing, testing, and maintaining the outsourced software application and infrastructure to the vendor, which should help IT managers eliminate routine tasks. This, in turn, will allow staff to dedicate more time to more strategic IT initiatives to add value to the business (Benlian & Hess, 2011).

Most cloud providers have recently changed their terms and conditions to specify the physical location of information in the cloud. These cloud providers are also seeking compliance to standards such as the Federal Information Security Management Act (FISMA) of 2002 and ISO27001 (Information Security Management) to prove their security credentials (Ferguson-Boucher & Convery, 2011).

Weaknesses. Security risks are possible since the SaaS and the data are hosted on external servers. SaaS clients give a provider control to their data without accurately knowing how the provider secures their data and which backup disaster recovery policies or procedures are in place. Also, technology advances so quickly which makes IT environments unpredictable (Benlian & Hess, 2011).

There are five factors to measure perceived risk for SaaS (Benlian & Hess, 2011):

- Performance – Addresses the possibility that SaaS won't perform as expected. SaaS may not provide application availability and/or bandwidth as the provider originally stated.
- Economic – Addresses the risk of the possibility that the client may have to incur more charges to reach a satisfactory level. SaaS's architectural approach shifts specific investments to the client such as customizing common code or data definitions on the provider's servers.
- Strategic – Addresses the risks that a company will lose critical resources and capabilities when using applications via SaaS. If a business moves a critical application that supports key functions to SaaS, then there is a heavy interdependence between the company and the external provider.
- Security – Address the security concern of a provider controlling company data without accurately knowing how the provider secures their data and which back up disaster recovery policies or procedures are in place.
- Managerial – Address the perceptions that SaaS may create since task or jobs may be viewed as outsourced to the SaaS provider. This can affect how managers are perceived by their co-workers, clients, and staff.

According to Da Veiga and Eloff (2010), two to three percent of an organization's annual profit may be lost due to information security incidents. Studies show that insiders pose the most threat to the information of an organization. Other research shows that insiders can be behind most of the breaches whether intentional or not. It can be argued that the goal of securing information is to a certain extent in conflict with the normal business goals of maximizing productivity and minimizing costs (Van Niekerk, & Von Solms, 2010).

A security aware culture within the organization is needed to guard against such breaches. The objective is to instill information security that conduces the protection of information assets based on the information security policies (Da Veiga & Eloff, 2010).

Opportunity. Technology from cloud computing such as virtualization can be used in-house to setup a private cloud (Ferguson-Boucher & Convery, 2011). According to Ferguson-Boucher & Convery (2011), it is expected that private cloud models will be adopted more in order to avoid possible information security risks such as multi-tenancy and distributed data centers.

The cloud will receive greater scrutiny and security. Organizations are experiencing growing use of mobile and cloud technologies for file sharing. Organizations see threats of these technologies if they go ungoverned. In 2013, organizations will increase their use of private or hybrid clouds to meet their mobile workforce needs (Shute, 2012).

Threats. Perhaps the biggest threat to adoptions of cloud computing is regulation at the local, national, and international level. This regulation can cover a range from data privacy and data access to compliance requirements and data location requirements. Regulation, such as Sarbanes-Oxley and the Health and Human Services Health Insurance Portability and Accountability Act (HIPPA), has requirements for physical data audits. Other regulations at the local, national and international level might negate the benefits of cloud computing, For example, many nations have laws requiring SaaS providers to keep customer data and copyrighted materials within national borders (Marston, Li, Bandyopadhyay, Zhang, & Ghalsasi, 2011). Policy factors are instrumental to the success of the cloud industry (Farrell, 2010). Farrell (2010) warns that the government should not overregulate or adapt existing regulations to this technology; rather the government should take a long-term view and enact forward-looking legislation which is global and cross-jurisdictional in nature.

As records move to the cloud, the ability to keep confidentiality may diminish to an unknown degree. Furthermore, when the aggregation of sensitive data is stored in large data centers it can increase the appeal for potential cybercriminals to attempt to steal the information (Devereaux & Gottlieb, 2012).

Information security consists of many processes in which some are dependent on human behavior. Employees are the greatest threat to information security either due to intention, lack of knowledge, or negligence. For this issue, many studies have shown that the establishment of an information security culture in an organization is necessary for effective information security (Van Niekerk, & Von Solms, 2010). According to Van Niekerk & Von Solms (2010), corporate culture exists on different levels:

- Level 1 - Artifacts – What can be seen, heard, and felt in an organization (i.e. visible organizational structures and processes).
- Level 2 – Espoused values – The reasons an employee would give for the observed artifact (i.e. documents that describe the company values).
- Level 3 – Shared tacit assumptions – Implied assumptions usually from beliefs and values that continue to be successful or from the company's early years.

In any information security culture a certain form of elasticity will be present. This elasticity will determine whether the tacit assumptions will over time align to the espoused values of the organization. With education aimed at improving employee attitudes towards information security, organizations can reduce the elasticity in the culture and speed up the pace at which measureable artifacts become more in line with the espoused values (Van Niekerk & Von Solms, 2010).

References

Aberystwyth University (n.d.). Kirsten Ferguson-Boucher. Retrieved June 7, 2013, from http://www.aber.ac.uk/en/dis/staff/knb/

AIIM (2013a). About AIIM. Retrieved from http://www.aiim.org/about

AIIM (2013b). What is information management? Retrieved from http://www.aiim.org/what-is-information-management

AIIM (2013c). What is electronic records management (ERM)? Retrieved April 30, 2013, from http://www.aiim.org/What-is-ERM-Electronic-Records-Management

AIP Conference Proceedings. (2013, May 31). In *Wikipedia, the free encyclopedia*. Retrieved from http://en.wikipedia.org/w/index.php?title=AIP_Conference_Proceedings&oldid=483081238

Alalwan, J., & Thomas, M. (2011). An ontology-based approach to assessing records management systems. *E-Service Journal*, *8*(3), 24.

Alexander, B. (n.d.). Institute for Information Systems and New Media - LMU Munich. Retrieved June 11, 2013, from http://www.en.wim.bwl.uni-muenchen.de/persons/lehrbeauftragte/benlian/index.html.

APA. (n.d.). About. Retrieved June 18, 2013, from http://www.apa.org/about/index.aspx

APJIS. (n.d.). *Asia Pacific Journal of Information Systems*. Retrieved June 16, 2013, from http://apjis.or.kr/

Application programming interface (n.d.). Wikipedia. Retrieved June 30, 2013, from http://en.wikipedia.org/wiki/Application_programming_interface

ARMA International (n.d) (a). What is records management? Retrieved from https://www.arma.org/pdf/whatisrim.pdf

ARMA International. (n.d.) (b) Who we are. Retrieved June 18, 2013, from http://www.arma.org/r2/who-we-are

Australasian Conference on Information Systems. (2013, March 14). In *Wikipedia, the free encyclopedia*. Retrieved from http://en.wikipedia.org/w/index.php?title=Australasian_Conference_on_Information_Systems&oldid=514384892

Barnes, F. R. (2010). Putting a lock on cloud-based information. *Information Management Journal*, *44*(4), 26–30.

Bathe, R., Jawale, V., & Jundre, V. (2013). Secure cloud based document management system. *International Journal of Engineering*, *2*(3). Retrieved from http://www.ijert.org/browse/volume-2-2013/march-2013-edition?download=2559%3Asecure-cloud-based-document-management-system&start=10.

Bell, C., & Frantz, P. (2012). Critical evaluation of information sources. *University of Oregon Libraries.* Retrieved May 1, 2013, from https://library.uoregon.edu/guides/findarticles/credibility.html

Benlian, A., & Hess, T. (2011). Opportunities and risks of software-as-a-service: Findings from a survey of IT executives. *Decision Support Systems*, *52*(1), 232–246. doi:10.1016/j.dss.2011.07.007

Berg, K. (2011). Federal Government enters the era of the "Cloud." *News Media & the Law*, *35*(4), 16–18.

Bibi, S., Katsaros, D., & Bozanis, P. (2012). Business application acquisition: On-premise or saas-based solutions? *IEEE Software*, *29*(3), 86–93. doi:10.1109/MS.2011.119

Breeding, M. (2013). Digital archiving in the age of cloud computing. *Computers in Libraries*, *33*(2), 22–26.

Brookings Institution. (n.d.). About Brookings. Retrieved June 15, 2013, from http://www.brookings.edu/about#research-programs/

Busch, C., De Maret, P., Flynn, T., Kellum, R., Le, S., Meyers, B, Saunders, M., White, R., Palmquist, M., (2012). Conceptual analysis. Writing@CSU. Colorado State University. Available at http://writing.colostate.edu/guides/guide.cfm?guideid=61

Cloud Provider. (n.d.). *Webopedia*. Retrieved May 1, 2013, from http://www.webopedia.com/TERM/C/cloud_provider.html

Cloud Security Alliance. (n.d.). Tim Grance. Retrieved June 9, 2013, from http://www.csathailand.org/Summit2013/Profiles/TimGrance.aspx

Cloud use can complicate e-discovery. (2013). *Information Management Journal*, *47*(1), 17–17.

Computers & Security Journal - Elsevier. (n.d.). Retrieved June 24, 2013, from http://www.journals.elsevier.com/computers-and-security

Convery, N. (n.d.). LinkedIn. Retrieved June 8, 2013, from http://www.linkedin.com/profile/view?id=66757993&authType=NAME_SEARCH&authToken=p10G&locale=en_US&srchid=1468052113706580048458&srchindex=1&srchtotal=3&trk=vsrp_people_res_name&trkInfo=VSRPsearchId%3A146805211370658004845%2CVSRPtargetId%3A66757993%2CVSRPcmpt%3Aprimary

Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers & Security*, *29*(2), 196–207. doi:10.1016/j.cose.2009.09.002

Devereaux, R. L., & Gottlieb, M. C. (2012). Record keeping in the cloud: Ethical considerations. *Professional Psychology: Research and Practice*, *43*(6), 627–632. doi:10.1037/a0028268

EDRMS. (2013, March 10). Electronic document and records management system. In *Wikipedia, the free encyclopedia*. Retrieved from http://en.wikipedia.org/w/index.php?title=Electronic_document_and_records_management_system&oldid=543147227

Elsevier. (2013, June 5). In *Wikipedia, the free encyclopedia*. Retrieved from http://en.wikipedia.org/w/index.php?title=Elsevier&oldid=557042635

Empel, S. (2012). How to evaluate new technologies for RIM impact. *Information Management Journal*, *46*(6), 36–40.

Farrell, R. (2010). Securing the cloud-governance, risk, and compliance issues reign supreme. *Information Security Journal: A Global Perspective*, *19*(6), 310–319.

Ferguson-Boucher, K., & Convery, N. (2011). Storing information in the cloud – A research project. *Journal of the Society of Archivists*, *32*(2), 221–239. doi:10.1080/00379816.2011.619693

Fraunholz, B. (n.d.). Biography. Retrieved June 11, 2013, from http://bardofraunholz.cgpublisher.com/biography.html

Foley, J. (2012, October 22). Expect to save millions in the cloud? Prove it. *InformationWeek*, (1347), 5.

Forrester. (n.d.). About. Retrieved June 17, 2013, from http://www.forrester.com/home#/aboutus

Forrester Research. (n.d.)(a). Liz Herbert. Retrieved June 16, 2013, from http://www.forrester.com/Liz-Herbert

Forrester Research. (n.d.) (b). Jon Erickson. Retrieved June 17, 2013, from http://www.forrester.com/Jon-Erickson

Fujitsu Global. (n.d.). Retrieved June 23, 2013, from http://www.fujitsu.com/global/news/publications/periodicals/fstj/

Gartner. (n.d.) (a). Cloud computing. *Gartner IT Glossary*. Retrieved April 29, 2013, from http://www.gartner.com/it-glossary/cloud-computing/

Gartner. (n.d.) (b). Software as a service (SaaS). *Gartner IT Glossary*. Retrieved April 29, 2013, from http://www.gartner.com/it-glossary/software-as-a-service-saas/

Hai, H. , Sakoda, S. , & Fujitsu, L. (2009). SaaS and integration best practices. *Fujitsu Scientific & Technical Journal*, *45*(3), 257-264.

Healey, M. (2010, May 17). Practical guide to saas success. *InformationWeek*, (1267), 40.

Herbert, L., Erickson, J. (2011). The ROI of cloud apps. *Forrester Research*. Retrieved from https://www.mercurymagazines.com/pdf/BOXNET3.pdf

Humphrey, A.S. (2005). SWOT analysis for management consulting. *SRI Alumni Association Newsletter*,December, 2005, 7. Retrieved from http://www.sri.com/sites/default/files/brochures/dec-05.pdf

IEEE Security and Privacy (n.d.). About IEE. Retrieved June 22, 2013, from http://www.computer.org/portal/web/computingnow/securityandprivacy/about

IEEE Transactions on Computers. About (n.d.). Retrieved June 26, 2013, from http://www.computer.org/portal/web/tc/about

IETE Technical Review. (n.d.). About us. Retrieved June 23, 2013, from http://tr.ietejournals.org/aboutus.asp

IJERT. (n.d.) International Journal of Engineering Research and Technology. Retrieved June 15, 2013. Retrieved from http://www.ijert.org/#

InformationWeek. (n.d.). John Foley Bio. Retrieved June 17, 2013, from http://www.informationweek.com/authors/John-Foley

Internet Librarian, (2012). Speaker Directory. Retrieved June 14, 2013, from http://www.infotoday.com/il2012/speakers.asp

Jansen, W., & Grance, T. (2011). Guidelines on security and privacy in public cloud computing. *NIST special publication*, *800*, 144.

JSTOR. (n.d.) e-Service Journal. Retrieved June 23, 2013, from http://www.jstor.org/page/journal/eservicej/forAuthor.html

Kamal, S., & Kaur, R. (2011). Cloud computing security issue: survey. *AIP Conference Proceedings*, *1414*(1), 149–153. doi:10.1063/1.3669947

Kaufman, L. M. (2009). Data security in the world of cloud computing. *IEEE Security Privacy*, *7*(4), 61–64. doi:10.1109/MSP.2009.87

Literature Reviews. (n.d.). *The Writing Center*. Retrieved May 6, 2013, from https://writingcenter.unc.edu/handouts/literature-reviews/

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing - The business perspective. *Decision Support Systems*, *51*(1), 176–189. doi:10.1016/j.dss.2010.12.006

McAffee. (2012). SaaS named most promising technology. Retrieved April 29, 2013, from http://www.mcafee.com/fr/solutions/cloud-security/news/20120822-03.aspx

Mell, P., & Grance, T. (2011). The NIST definition of cloud computing. *NIST special publication*, *800*, 145.

Multitenancy. (2013, June 22). In *Wikipedia, the free encyclopedia*. Retrieved from http://en.wikipedia.org/w/index.php?title=Multitenancy&oldid=560653642

NARA. (n.d.). What is the National Archives and Records Administration? *National Archives*. Retrieved May 11, 2013, from http://www.archives.gov/about/

Nguyen, L. T., Swatman, P. M. C., & Fraunholz, B. (2007). EDMS, ERMS,ECMS or EDRMS: fighting through the acronyms towards a strategy for effective corporate records management. *ACIS2007 Toowoomba 5 to 7 December 2007 [electronic resource] : proceedings of the 18th Australasian conference on information systems*, 790–800.

Orlando, D. (2011). Cloud computing service models, Part 3: Software as a service. *IBM DeveloperWorks* (2011, January 31). Retrieved April 30, 2013, from http://www.ibm.com/developerworks/cloud/library/cl-cloudservices3saas/

Project MUSE. (n.d.). Retrieved June 23, 2013, from http://muse.jhu.edu/

Records Manager. (n.d.). *AmDoc Glossary of Terms*. Retrieved April 23, 2013, from website: http://www.expertglossary.com/ediscovery/definition/records-manager

Records Update. (n.d.). About us. Retrieved June 10, 2013, from http://www.recordsupdate.com/about.cfm

Reporters Committee for Freedom of the Press. (n.d.). Reporters Committee for Freedom of the Press. (n.d.).

US Department of Commerce. (n.d.). NIST general information. Retrieved April 29, 2013, from http://www.nist.gov/public_affairs/general_information.cfm

Sehgal, N. K., Sohoni, S., Ying Xiong, Fritz, D., Mulia, W., & Acken, J. M. (2011). A Cross Section of the Issues and Research Activities Related to Both Information Security and

Cloud Computing. *IETE Technical Review*, *28*(4), 279–291. doi:10.4103/0256-4602.83549

Shum, W. (2013, January 8). State of Oregon embraces HP TRIM for statewide cloud-based records management program.). *Reuters*. Retrieved from http://www.reuters.com/article/2013/01/08/ca-hp-trim-autonomy-idUSnPnSF38775+160+PRN20130108

Shute, W. (2012). Information governance takes center stage in 2013: Spotlight shines on IG pros. *Information Management Journal, 46*(6), 22–25.

Society of American Archivists. (n.d.). About SAA. Retrieved April 29, 2012, from http://www2.archivists.org/about

Software as a service. (2013, May 3). In *Wikipedia, the free encyclopedia*. Retrieved from http://en.wikipedia.org/w/index.php?title=Software_as_a_service&oldid=553347271

State Records NSW. (n.d.). Record keeping in brief 61 - FAQs about EDRMS. Retrieved April 30, 2013, from http://www.records.nsw.gov.au/recordkeeping/government-recordkeeping-manual/guidance/recordkeeping-in-brief/recordkeeping-in-brief-61#what-is-an-edrms-

Swatman, P. (n.d.). LinkedIn. Retrieved June 11, 2013, from http://www.linkedin.com/profile/view?id=3204636&authType=NAME_SEARCH&authToken=3NYq&locale=en_US&srchid=1468052113709O7262309&srchindex=1&srchtotal=5&trk=vsrp_people_res_name&trkInfo=VSRPsearchId%3A146805211370907262309%2CVSRPtargetId%3A3204636%2CVSRPcmpt%3Aprimary

SWOT analysis. (2013, April 24). In *Wikipedia, the free encyclopedia*. Retrieved from http://en.wikipedia.org/w/index.php?title=SWOT_analysis&oldid=551917349

Symons, C. (2008). Justifying and funding infrastructure investments. *Forrester*. Retrieved from http://zimmer.csufresno.edu/~sasanr/Teaching-Material/MIS/SDLC/Justifying%20&%20Funding%20Infrastructure%20Investments.pdf

Tak, B. C., Urgaonkar, B., & Sivasubramaniam, A. (2013). Cloudy with a chance of cost savings. *IEEE Transactions on Parallel and Distributed Systems*, *24*(6), 1223–1233. doi:10.1109/TPDS.2012.307

Taylor & Francis. (2013, May 31). In *Wikipedia, the free encyclopedia*. Retrieved from https://en.wikipedia.org/w/index.php?title=Taylor_%26_Francis&oldid=556096970

The Seybold Report. (n.d.). About. Retrieved June 22, 2013, from http://www.seyboldreport.com/about.html

Thomson Reuters. (n.d.). About us. Retrieved June 16, 2013, from http://thomsonreuters.com/about-us/

Tolliver-Nigro, H. (n.d.). Retrieved June 22, 2013, from http://www.digitalprintingreports.com/aboutheiditolliv.html

Tolliver-Nigro, H. (2009). SaaS 101: The basics of software as a service. *Seybold Report: Analyzing Publishing Technologies*, *9*(15), 3–8.

Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security*, *29*(4), 476–486. doi:10.1016/j.cose.2009.10.005

Virtualization (n.d.). Wikipedia. Retrieved July 3, 2013, from http://en.wikipedia.org/wiki/Virtualization

West, D. M. (2010). Saving money through cloud computing. *Governance Studies at Brookings*. Retrieved from http://www.brookings.edu/~/media/research/files/papers/2010/4/07-cloud-computing-west/0407_cloud_computing_west.pdf

West, D.M. (n.d.). *The Brookings Institution*. Retrieved June 15, 2013, from http://www.brookings.edu/experts/westd

Whitman, M.E., & Mattord, H.J. (2010). Management of information security. Boston, MA: Course Technology Cengage Learning.

Yang, S., Yoo, B., Jahng, J. (2010). Does the saas model really increase customer benefits? *Asia Pacific Journal of Information Systems*. Retrieved from http://apjis.or.kr/pdf/MIS020-002-5.pdf

Zotero. (n.d.) About. Retrieved from http://www.zotero.org/about/