Enhancing Cloud Security and Privacy: Broadening the Service Level Agreement

Bob Duncan
Computing Science
University of Aberdeen
Email: bobduncan@abdn.ac.uk

Mark Whittington
Accounting and Finance
University of Aberdeen
Email: mark.whittington@abdn.ac.uk

***Abstract*—Achieving security and privacy in the cloud is not a trivial exercise. Indeed, the difficulties associated with achieving this goal are both many and highly complex, and present one of the major barriers to the uptake of cloud computing. Yet, we know cloud computing offers the possibility of substantial economic benefit to firms, as well as providing great agility, which can offer a competitive advantage in today's difficult trading conditions. We address this issue by considering whether greater accountability, and particularly a broadening of the scope of Service Level Agreements, can enhance cloud security and privacy.**

***Index Terms*—security; privacy; standards; compliance; assurance; audit; service level agreements; cloud service providers; responsibility; accountability; agency theory; stewardship theory**

I. Introduction

What do we mean by cloud security and privacy? A fundamental requirement of achieving privacy is to first have a proper level of security. Without security, there can be no privacy. Thus we must first consider the issues of achieving proper security. The Oxford English Dictionary (OED) [1] has two useful definitions of security "The safety of an organization, establishment, or building from espionage, criminal activity, illegal entrance or escape, etc." and "With reference to cyber-security: the state of being protected against the criminal or unauthorized use of electronic data, or the measures to achieve this." Privacy, OED: "absence or avoidance of publicity or display; secrecy, concealment, discretion; protection from public knowledge or availability", is clearly linked to security. It is, however, difficult for a company to know if it is secure, especially as this is likely to be a moving target over time and be affected by changes in internal processes or the outside environment. The company's management can seek to assure itself of security through assurance, OED: "A promise or engagement making a thing certain; a formal engagement, pledge, or guarantee; a positive declaration intended to give confidence", through employing individual or corporate experts to interrogate the company's processes and internal activities. A key part of this assurance could come from trust in a broad written agreement between provider and user (usually referred to as the "Service Level Agreement" in a cloud context) that was open to regular and thorough inspection and verification. In this paper we contend that "SLA's" are too narrow in scope and too one-sided in nature for such user confidence to be established.

This evidence can take two forms: compliance or audit. Compliance, OED: "The action or fact of complying with a wish or command", requires a code or set of standards against which the company's activities and processes can be compared and either match (compliant) or fall short (non-compliant). The evidence of security that a compliance check list provides depends on a number of factors including the knowledge and independence of those who wrote the code and whether it is still pertinent to today's environment.

Audit, OED: "To make an official systematic examination of (accounts), so as to ascertain their accuracy", requires outsiders who are deemed to be both objective and expert to form their own opinion of what is being examined and then to publicly state their confidence (or otherwise) in the reliability of what they have investigated. Auditing is not straightforward or easy. Just as with accounting auditors, objectivity is difficult when companies pay auditors who would like to be retained for the following year. Audit is also potentially very expensive if done well by the best experts in the field and there is a temptation to reduce the experts' role to one of advising, often writing checklists to be administered by qualified technicians.

The remainder of the paper is organized as follows: in Section II we discuss the challenges of cloud security and privacy, including the definition of a set of security goals, compliance with cloud security standards, audit issues, the impact of management approaches on security, and how complexity and the lack of responsibility and accountability affects cloud security; In Section III we investigate why these challenges are difficult to address; In Section IV we address the remaining key issue to be tackled; and in Section V our conclusions.

II. The Challenges

There are a number of challenges which need to be addressed in order to achieve the goal of good security. The fundamental concepts of information security are confidentiality, integrity, and availability (CIA), a concept developed when it was common practice for corporate management to run a company under agency theory. Agency theory can be used to describe a contract under which the principal engages an agent to perform some service on their behalf which involves delegating some decision making authority to the agent. Shareholders (principal) and chief executive officer (agent) is one such relationship. While both principal and agent are

978-1-4673-7952-6/15 $31.00 © 2015 IEEE
DOI 10.1109/Trustcom-BigDataSe-ISPA.2015.487

utility maximisers, they would not necessarily always have the same alignment of goals. We have all seen how the excesses of corporate greed have failed to be curtailed by agency theory. The same is true for cloud security, which would suggest a different approach is needed. The rest of the paper addresses the following important points in turn: Definition of security goals; Compliance with standards; Audit issues; Management approach; Complexity; Lack of responsibility and accountability.

A. Definition of Security Goals

The business environment is constantly changing, as are corporate governance rules, with more emphasis now being placed on responsibility and accountability [2], social conscience [3], sustainability [4][5], resilience [6] and ethics [7]. Responsibility and accountability are, in effect, mechanisms we can use to help achieve all the other security goals. Since social conscience and ethics are very closely related, the traditional CIA triad can be expanded to include sustainability, resilience and ethics.

In this enhanced security requirements framework, we note definitions of the added factors: Sustainability, OED: "the quality of being sustainable at a certain rate or level". Resilience, OED: "the quality or fact of being able to recover quickly or easily from, or resist being affected by, a misfortune, shock, illness, etc.; robustness; adaptability". Ethics, OED: "the codes of conduct or moral principles recognized in a particular profession, sphere of activity, relationship, or other context or aspect of human life". We include social responsibility under this heading which can be defined as "the practice of producing goods and services in a way that is not harmful to society or the environment".

B. Compliance with Standards

Looking at how we achieve these goals in practice, we have identified the use of assurance to achieve security through compliance and audit. Turning first to compliance, there are a number of challenges to address. Since the evolution of cloud computing, there are a number of cloud security standards which have evolved, but the problem is that there is still no standard which offers a comprehensive level of complete security — there is no "one size covers all", which is a limitation. Even compliance with all standards will not guarantee complete security, which, presents another disadvantage [8].

While standards compliance is often perceived as a laudable aim, the flaw where new computing technology is concerned is that the pace of evolution of new technology far outstrips the capability of international standards organisations to keep up with the changes [9]. This slow pace of evolution of cloud security standards presents a major flaw in a rapidly evolving technological and threat landscape, with the potential to cause immeasurable harm to companies. A further flaw with compliance mechanisms used in cloud security standards is the manner in which checklists are used [10]. Compliance with security standards can be viewed as an agency reaction by company management to protect them from being sued by their own principals for failing to implement proper security. Since current standards are neither complete, nor up to date, compliance with these standards cannot ensure security [8].

Compliance audit frequency is generally quite relaxed. Reassessment need take place only when system changes take place, or every few years, otherwise. This completely fails to grasp the rapidly evolving nature of security threats. There exists a clear need to employ some method of continuous monitoring when it comes to security management. Reports from global security companies [11]–[13] suggest that over 85% of security breaches involve a low level of technical competence, facilitated instead by lack of understanding, lack of competence, or poor configuration of victims' systems.

C. Audit Issues

Auditing in the accountancy world has enjoyed the benefit of over a century of practice and experience, yet there remain differences of opinion with a number of problems yet to be resolved. Duncan and Whittington [8] provide some background on this issue. Cloud computing audit is not a mature field, and there will be some way to go before it can catch up with work done in the accounting profession. An obvious area of weakness arises when taking audit professionals from the accounting world out of their comfort zone, and placing them in a more technical field. Equally, the use of people with a computing background can overcome some of these issues, but their lack of audit background presents another weakness. Gray et al [14] address corporate social reporting considering the concepts of accountability and the social contract. Gray [15] considers accounting's potential for contribution to accountability and transparency in participative democracy, the potential for non-financial accounts of the biosphere and, perhaps most contentiously, the use of current accounting techniques for the operationalisation of an accounting for sustainability. Dhillon and Backhouse [16] suggest that in addition to traditional CIA security concerns, organisations must consider that responsibility, integrity, trust and ethicality principles hold the key for successfully managing information security.

Gray [17], considers the previous 30 years of social accounting, reporting and auditing, and proposes that this is the function of accountability — to require individuals and organisations to present an account of those actions for which society holds them — or would wish to hold them — responsible. Owen et al [18] suggest that despite seemingly endorsing active stakeholder engagement, current social and ethical accounting, auditing and reporting practice amounts to little more than corporate spin. Alles et al [19] consider the feasibility and economics of continuous assurance. Cohen et al [20] recognise the importance of corporate governance in ensuring sound financial reporting and deterring fraud. They found that auditors view management as the primary driver of corporate governance.

Ramamoorti [21] considers the establishment, growth, and evolution of the contemporary internal auditing profession. Adams and Evans [22] address concerns in achieving greater

accountability in social reports. Moeller [23] considers how the role of internal audit has changed since the introduction of SOX in 2002. Zeff [24] examines the historical evolution in the US of the use of the term "present fairly" in the auditor's report. Archambeault et al [25] consider the need for an IAR to increase governance transparency for external stakeholders, to complement existing governance disclosures, increase stakeholder confidence in governance quality, and motivate internal audit diligence, while recognising that further research is needed.

Cloud audit research has been limited due to a combination of the lack of maturity in the field and the greater technical complexities posed. Bernstein et al [26] in their proposed framework for promoting trust in the use of cloud systems identified the need to ensure a proper audit trail is maintained. Leavitt [27] warns that companies will be unable to pass audit by their customers if they are unable to demonstrate an adequate level of control over cloud data. Chen et al [28] propose the novel concept of mutual audit as a means of improving trust between parties. Pearson and Benameur [29] consider the use of tracing audit authorities to enhance privacy, security and trust. Zhou et al [30] propose an extra audit layer to be run on the cloud to "watch over" what goes on in the cloud.

Ramgovind et al [31] note that reluctance of cloud vendors to allow audit, or to undergo standards compliance presents a barrier to use. IsecT [32] present a superficial introduction to information security frameworks, covering security standards, laws, regulations and security recommendations or obligations of various kinds. Hoyer et al [33] suggest a generic architectural model to unify the classic fraud audit approach with human behaviour in order to achieve better fraud detection and prevention. Ko et al [34] note that despite audit-ability being one the key components of trust, most of the cloud service providers (CSP) are failing to address the issue, while noting the difficulties present in achieving such a goal. Brucker et al [35] present a tool chain to support both design-time modelling as well as run-time enforcement of security requirements for business process-driven systems. Stahl et al [36] carry out a critical evaluation of information security policies in the UK healthcare sector.

De Haes et al [37] suggest COBIT could make a good framework for the enterprise governance of IT. Mulig et al [38] note that in many companies, accounting departments deal with downloaded data that is analysed using worksheet software, which can bypass normal IT controls. Herath and Herath [39], addressing compliance with ever-increasing privacy laws, accounting and banking regulations, and standards, suggest this is top priority for most organisations, but express concern that, unlike financial reporting, information security and systems audits are not mandatory.

D. Management Approach

CSPs have developed their cloud business models using agency theory. Pallas et al [40] suggest that agency theory models the current relationship between CSPs and cloud users very well, further suggesting this expresses all the weaknesses of agency and highlights many of the issues still faced today. Given the potential multiplicity of actors, and the complexities of their relationships with each other in cloud ecosystems, it is clear that simple traditional agency relationships (where each actor looks to their own short term ends) will no longer be able to handle fully the security implications for users of these ecosystems. There is a clear need for developing a stronger mechanism to ensure users of such ecosystems can be assured of the security of their information. The question is, how does management approach impact on cloud security?

Standard service level agreement (SLA) offerings from the major players basically ignore accountability, assurance, audit, confidentiality, compliance, integrity, privacy, responsibility and security, merely offering availability as the focus of their measure of performance. The onus for measuring and proving unacceptable performance is neatly passed to the customer, which, with the inclusion of some suitably deeply buried clauses in the small print, assures the buck invariably never stops with the CSP. Of course it is possible to negotiate an SLA to include these missing measures, but one would anticipate that the arrangement costs and increased service costs would significantly reduce or even eliminate any potential cost savings offered by the cloud paradigm. Since such costs would, in any event, only be affordable by the largest corporations, this puts most small and medium-sized enterprises (SME) and sole traders at a commercial disadvantage.

This is clearly worrying in today's climate of increasing punitive regulatory fines for privacy and security breaches and the potential negative impact on business costs and the knock-on negative impact on share values. Taken against a backdrop of an ever expanding threat environment, it is clear that positive action is needed globally.

E. Complexity

Another issue is the increasing complexity which new technology brings, and the ever increasing potential exposure to risk brought about by a failure to grasp the significance of risks arising as a result of this increase in complexity [41]. Traditional distributed information systems present a multiplicity of technical layers, each of which must interact with one or more other layers. Rather than simplifying this process, cloud introduces yet more layers. There is Infrastructure, Platform and Software as a Service (IaaS, Paas and SaaS), each of which can be operated by different actors. Cloud brokers may also be involved, leading to yet more layers, yet more complexity, yet more risk. Thus, there is a need for a more agile, effective, approach to address these issues. Another hurdle to be overcome is the cross disciplinary nature of today's corporate world, with more cross-over between disciplines than in the past, which means no single discipline can effectively deal with all the issues arising from the use of cloud technology [42]. Existing security paradigms have not kept pace with the rapidity of development, change and complexity in modern information ecosystems. There is a danger that continued reliance on existing models will lead to real weaknesses in

systems which can be vulnerable to exploitation. The challenge here is to develop a means of addressing these weaknesses at a conceptual level which can be demonstrably more robust than existing mechanisms currently in place. We aim to address this challenge in our future work.

F. Lack of Responsibility and Accountability

We must also consider the role that responsibility and accountability play in achieving this difficult objective. Responsibility, OED:"a moral obligation to behave correctly towards or in respect of a person or thing", Accountability, OED: "the quality of being accountable; liability to account for and answer for one's conduct, performance of duties, etc. (in modern use often with regard to parliamentary, corporate, or financial liability to the public, shareholders, etc.)". Monahan and Yearworth [43] observe that SLAs should be meaningful, both for customers and vendors as defined by some objective criteria, but evidence from procurement failures for large IT systems suggests otherwise. This observation has inspired an investigation into the possibility of offering alternative security SLAs that would be meaningful to both customers and vendors. Yao et al [44] consider the implementation of an Accountability as a Service approach using continuous cloud monitoring and audit to ensure better quality of service. Haeberlen et al [45] propose that cloud services should be mutually accountable to both CSP and customer, to ensure a proper level of service can be achieved, however did accept that some challenges remain to be overcome.

The Cloud Accountability Project (A4Cloud) focuses on: "The Accountability For Cloud and Other Future Internet Services as the most critical prerequisite for effective governance and control of corporate and private data processed by cloud-based IT services". Pearson et al [46] write about the A4Cloud project which has as its main focus accountability. By combining methods of risk analysis, policy enforcement, monitoring and compliance auditing with tailored IT mechanisms for security, assurance and redress, A4Cloud aims to extend accountability across entire cloud service value chains, covering personal and business sensitive information in the cloud. Catteddu et al [47] present a model of accountability for cloud computing services, based on ongoing work as part of the A4Cloud project. Theoharidou et al [48] examine privacy risk assessment for cloud, and identify threats, vulnerabilities and countermeasures that clients and providers should implement in order to achieve privacy compliance and accountability.

Hon et al [49] consider the implications for cloud accountability of current proposals under the draft General Data Protection Regulation to modernise the EU Data Protection Directive. Bernsmed et al [50] identify and explore a number of accountability obligations that arise in the context of medical sensor networks in the cloud, including accountability obligations from a European perspective. Ko [51] reviews the definitions, existing techniques and standards in the area of data accountability in cloud computing. Benghabrit et al [52] propose a framework for the representation of cloud accountability policies. Tountopoulis et al [53] elaborate on the general aspects of an accountability-based approach to IT and data governance, which can facilitate organisations dealing with the cloud to comply with applicable legislation and provide more evidence that confidential and/or personal data are handled in accordance with relevant data protection legislation. Papanikolaou et al [54] present an implemented system to model and visually represent the functioning of accountability mechanisms for cloud computing (such as policy enforcement, monitoring, intrusion detection, logging, redress and re-mediation mechanisms) over provider boundaries along the supply chain of service providers.

It is clear that the rapid evolution of the cloud computing paradigm has been facilitated by the agency approach of all the CSPs. While this has resulted in a rapid and successful implementation of a highly attractive new paradigm, it has also glossed over a myriad issues relating to proper security and privacy, concerns which are justifiably gaining far more traction in today's highly dangerous security environment.

III. Why These Challenges are Difficult to Address

The fundamental security concepts of CIA are no longer enough to cope with today's corporate responsibilities. In an environment where corporate governance extends far beyond these basic requirements, more is needed. With Pym, we have suggested [55] that the traditional CIA approach be expanded to cover sustainability, resilience and ethics, in order to more properly reflect today's changed corporate governance environment. We have warned of the dangers surrounding compliance with standards [8], and the mechanisms deployed for compliance [10]. We suggest that compliance with standards, in a world where security goals are a constantly moving target, where standards are incomplete, out of date, not fully relevant or otherwise inappropriate, will not be a trivial exercise.

The challenge of dealing with audit remains complex, and all the more difficult where CSPs are neither willing to allow proper audit trail recording to be carried out, nor to allow third parties to audit their systems. We suggest that this issue will become much easier to address if the issue of responsibility and accountability is first resolved. This is an area for further research. The existing agency theory-based management approach presents a serious challenge in the complex ecosystem of the cloud. The unwillingness of CSPs to accept responsibility for their part in ensuring a proper level of cloud security and privacy is a critical issue. We have proposed [56] that a move away from agency theory towards stewardship theory may go some way towards helping rectify this situation. Under stewardship theory, the behaviour of a steward is collective. This behaviour is closely aligned with the success of the organisation.

Companies are quite properly legally held responsible and accountable to a variety of regulators throughout industry under privacy and security regulations. Fines for non-compliance are reaching punitive levels, and many regulators have extreme levels of sanction at their disposal. Yet, where such companies

use cloud, the CSPs are not held to account for their role in such failures! Little wonder there is so much resistance to the adoption of this resource over fears of poor security and privacy. Cloud security standards organisations have tried for years to encourage CSPs to help lead development of proper cloud security standards by taking an active role in the process, and to accept responsibility for their part in achieving this goal. So far, they have been met with a resounding silence. However, this may be changing. In 2012, the European Commission (EC) published a cloud computing strategy [57], which outlines three objectives to encourage the use of cloud services, including the development of standard contractual terms for SLAs. The Commission published guidelines [58] developed by a sub-group of the Cloud Select Industry Group (CSIG) composed of representatives from expert groups such as the EU Agency for Network and Information Security (ENISA) and industry majors such as Amazon, Google, IBM, Microsoft, SAP and Salesforce, addressing areas of performance, security, data management and data protection.

While this impressive range of effort is welcomed, there are some issues. First, the guidelines are voluntary, rather than mandatory, which presents a fundamental flaw. Second, such guidelines would need to be developed at an international level to ensure effective enforcement across multiple jurisdictions. Third, some aspects of the guidelines are vague, and of course, they have yet to be trialed.

IV. Cloud Service Provider or Partner?

Given the nature of the rapidly evolving threat environment, and society's dependence on information systems, we suggest the time for serious action is already overdue, particularly on security and privacy. Cloud computing has the potential to become a fabulous resource for society as a whole, alongside business and government. Taking a fully accountable and ethical view of their responsibilities would assist CSPs to substantially open up the market for cloud computing and would improve their standing in the global community. CSPs need to provide a standard SLA that covers not only availability to the level they currently offer, but need to properly address issues of accountability, assurance, audit, confidentiality, compliance, integrity, privacy, responsibility and security.

Many of these issues can be more readily addressed using technical solutions, which would be relatively simple for CSPs to introduce. But, before this is possible, there is a need to accept responsibility for the service they offer, become accountable for their actions, or inactions, and to behave in a more complete, ethical manner towards cloud users. There is a huge potential market for the expansion of cloud computing from businesses, governments and individuals alike who are put off by the lack of accountability, assurance, audit, confidentiality, compliance, integrity, privacy, responsibility and security. CSPs have a golden opportunity to seize the initiative to radically transform the shape of cloud computing for the better. Hence the idea of the CSP being a "partner" with shared responsibility rather than a mere provider. This might reflect a more constructive level of relationship.

The work undertaken by the EU could provide a useful springboard for the rapid development of an ISO standard on cloud SLAs. Full international agreement and mandatory implementation would go a long way towards addressing this problem area. However, should CSPs persist in their refusal to address these key areas of accountability, assurance, audit, confidentiality, compliance, integrity, privacy, responsibility and security, then society as a whole will need to do something about it. Governments are not overly keen to introduce legislation, or regulation to such a technical industry. Self regulation would be a better approach for everyone. However, should there be no change to the status quo in the near future, perhaps regulators could start by forcing accountability on CSPs using existing powers with resulting bad publicity and possibly fines for non-compliance.

V. Conclusion

There is a clear need for better responsibility and accountability across all the actors involved in cloud ecosystems. CSPs persist in behaving with too great a level of self-interest and fail to accept broader responsibilities, resulting in cloud users having to bear the burden of this inequity between the parties. An initial step would be for the CSPs to take responsibility for their actions by including a proper provision for accountability in their SLAs. This will provide the basis for developing a level playing field between all cloud users and the CSPs.

Accountability will not guarantee complete security, but will assist in fairly sharing the risks between CSPs and cloud users. With accountability, technical solutions which have been developed up to now, will actually have a greater chance of working. Clearly, acknowledgement of assurance, audit, confidentiality, compliance, integrity, privacy and security in CSPs' SLAs, and specified to meaningful levels, would be signs of a welcome maturity of approach enabling and encouraging further acceptance and development.

References

[1] OED, "Oxford English Dictionary," 2014. [Online]. Available: www.oed.com

[2] M. Huse, "Accountability and Creating Accountability: a Framework for Exploring Behavioural Perspectives of Corporate Governance," *British Journal of Management*, vol. 16, no. s1, pp. S65–S79, Mar. 2005.

[3] A. Gill, "Corporate Governance as Social Responsibility: A Research Agenda," *Berkeley J. Int'l L.*, vol. 26, no. 2, p. 452, 2008.

[4] C. Ioannidis, D. Pym, and J. Williams, "Sustainability in information stewardship: Time Preferences, Externalities and Social Co-Ordination," in *WEIS 2013*, 2013, pp. 1–24.

[5] A. Kolk, "Sustainability, Accountability and Corporate Governance: Exploring Multinationals' Reporting Practices," *Business Strategy and the Environment*, vol. 17, no. 1, pp. 1–15, 2008.

[6] I. F. Stuart Chapin, G. P. Kofinas, and C. Folke, *Principles of Ecosystem Stewardship: Resilience-Based Natural Resource Management in a Changing World*. Springer, 2009.

[7] S. Arjoon, "Corporate Governance: An Ethical Perspective," *Journal of Business Ethics*, vol. 61, no. 4, pp. 343–352, Nov. 2005.

[8] B. Duncan and M. Whittington, "Compliance with Standards, Assurance and Audit: Does this Equal Security?" in *Proceedings of the 7th International Conference on Security of Information and Networks*. Glasgow: ACM, 2014, pp. 77–84.

[9] G. T. Willingmyre, "Standards at the Crossroads," *StandardView*, vol. 5, no. 4, pp. 190–194, 1997.

[10] B. Duncan and M. Whittington, "Reflecting on Whether Checklists Can Tick the Box for Cloud Security." in *Cloud Computing Technology and Science (CloudCom), 2014 IEEE 6th International Conference*. Singapore: IEEE, 2014, pp. 805–810.

[11] PWC, "UK Information Security Breaches Survey - Technical Report 2012," PWC2012, Tech. Rep. April, 2012.

[12] Trend, "2012 Annual Security Roundup: Evolved Threats in a "Post-PC" World," Trend Micro, Tech. Rep., 2012.

[13] Verizon, "2012 Data Breach Investigation Report: A study conducted by the Verizon RISK Team in cooperation with the United States Secret Service and Others," Tech. Rep., 2012.

[14] R. Gray, D. Owen, and K. Maunders, "Corporate social reporting: emerging trends in accountability and the social contract," *Accounting, Auditing \& Accountability Journal*, vol. 1, no. 1, pp. 6–20, 1988.

[15] R. Gray, "Accounting and environmentalism: an exploration of the challenge of gently accounting for accountability, transparency and sustainability," *Accounting, Organizations and Society*, vol. 17, no. 5, pp. 399–425, 1992.

[16] G. Dhillon and J. Backhouse, "Security Management in the New Millennium," *Comms. of the ACM*, vol. 43, no. 7, pp. 125–128, 2000.

[17] R. Gray, "Thirty years of social accounting, reporting and auditing: what (if anything) have we learnt?" *Business Ethics: A European Review*, vol. 10, no. 1, pp. 9–15, 2001.

[18] D. L. Owen, T. Swift, and K. Hunt, "Feature article Questioning the role of stakeholder engagement in social and ethical accounting , auditing and reporting *," *Accounting Forum*, vol. 25, no. No 3, pp. 264–282, 2001.

[19] M. G. Alles, A. Kogan, and M. a. Vasarhelyi, "Feasibility and Economics of Continuous Assurance," *AUDITING: A Journal of Practice & Theory*, vol. 21, no. 1, pp. 125–138, Mar. 2002.

[20] J. Cohen, G. Krishnamoorthy, and A. M. Wright, "Corporate Governance and the Audit Process," *Contemporary Accounting Research*, vol. 19, no. 4, pp. 573–594, 2002.

[21] S. Ramamoorti, "Internal Auditing: History, Evolution, and Prospects," *Research opportunities in internal auditing*, pp. 1–23, 2003.

[22] C. A. Adams and R. Evans, "Accountability, Completeness, Credibility and the Audit Expectations Gap," *Journal of corporate citizenship*, vol. 14, no. Summer, pp. 97–115, 2004.

[23] R. Moeller, "Managing internal auditing in a post-SOA world," *Journal of Corporate Accounting & Finance*, vol. 15, no. 4, pp. 41–45, 2004.

[24] S. Zeff, "The Primacy of "Present Fairly" in the Auditor's Report," *Accounting Perspectives*, vol. 6, no. 1, pp. 1–20, Mar. 2007.

[25] D. S. Archambeault, F. T. DeZoort, and T. P. Holt, "The Need for an Internal Auditor Report to External Stakeholders to Improve Governance Transparency," *Acct. Horiz.*, vol. 22, no. 4, pp. 375–388, Dec. 2008.

[26] D. Bernstein, S. Diamond, and M. Morrow, "Blueprint for the Intercloud Protocols and Formats for Cloud Computing Interoperability," in *Internet and Web Applications and Services, 2009. ICIW'09. Fourth International Conference on*, 2009, pp. 328–336.

[27] N. Leavitt, "Is Cloud Computing Really Ready for Prime Time?" *Computer*, vol. 42, no. January, pp. 15–20, 2009.

[28] Y. Chen and R. Sion, "On Securing Untrusted Clouds with Cryptography," *Science*, pp. 109–114, 2010.

[29] S. Pearson and A. Benameur, "Privacy, Security and Trust Issues Arising from Cloud," in *2nd IEEE International Conference on Cloud Computing Technology and Science, CloudCom 2010 (2010)*, no. Dec., 2010, pp. 693–702.

[30] W. Zhou, M. Sherr, W. R. Marczak, Z. Zhang, T. Tao, B. thau Loo, and I. Lee, "Towards a Data-centric View of Cloud Security," *Challenges*, pp. 25–32, 2010.

[31] S. Ramgovind, E. Mm, and E. Smith, "The Management of Security in Cloud Computing," in *Information Security for South Africa (ISSA), 2010*, 2010, pp. 1–7.

[32] IsecT, "Information security compliance," no. March, pp. 1–10, 2011.

[33] S. Hoyer, H. Zakhariya, T. Sandner, and M. H. Breitner, "Fraud prediction and the human factor: An approach to include human behavior in an automated fraud audit," *Proceedings of the Annual Hawaii International Conference on System Sciences*, pp. 2382–2391, 2011.

[34] R. K. L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, B. S. Lee, and Q. Liang, "TrustCloud: A Framework for Accountability and Trust in Cloud Computing," *Perspective*, pp. 1–9, 2011.

[35] A. D. Brucker, I. Hang, G. Lückemeyer, and R. Ruparel, "SecureBPMN: modeling and enforcing access control requirements in business processes," in *Proceedings of the 17th ACM symposium on Access Control Models and Technologies*, 2012, pp. 123–126.

[36] B. C. Stahl, N. F. Doherty, and M. Shaw, "Information security policies in the UK healthcare sector: A critical evaluation," *Information Systems Journal*, vol. 22, pp. 77–94, 2012.

[37] S. De Haes, W. Van Grembergen, and R. S. Debreceny, "COBIT 5 and Enterprise Governance of Information Technology: Building Blocks and Research Opportunities." *Journal of Information Systems*, vol. 27, no. 1, pp. 307–324, 2013.

[38] L. Mulig, S. Conger, and S. Conger, "Linking IS Audit Concepts to the Real World Via an Experiential Learning Exercise," in *The 5th Annual General Business Conference*, Huntsville, TX, 2013, pp. 1–12.

[39] H. S. Herath and T. C. Herath, "IT security auditing: A performance evaluation decision model," *Decision Support Systems*, vol. 57, pp. 54–63, Jan. 2014.

[40] F. Pallas, "An Agency Perspective to Cloud Computing," in *Economics of Grids, Clouds, Systems, and Services*. Springer, 2014, pp. 36–51.

[41] E. Zio, "Reliability engineering: Old problems and new challenges," *Reliability Engineering & System Safety*, vol. 94, no. 2, pp. 125–141, Feb. 2009.

[42] M. Dlamini, J. Eloff, and M. Eloff, "Information security: The moving target," *Computers & Security*, vol. 28, no. 3-4, pp. 189–198, May 2009.

[43] B. Monahan and M. Yearworth, "Meaningful security SLAs," HP Labs, Bristol, Tech. Rep., 2008. [Online]. Available: http://www.hpl.hp.com/techreports/2005/HPL-2005-218R1.pdf

[44] J. Yao, S. Chen, C. Wang, D. Levy, and J. Zic, "Accountability as a service for the cloud: From concept to implementation with BPEL," in *Proc. - 2010 6th World Cong. on Srvs., Srvs.-1 2010*, 2010, pp. 81–88.

[45] A. Haeberlen, "A Case for the Accountable Cloud," *ACM SIGOPS Operating Systems Review*, vol. 44, no. 2, pp. 52–57, 2010.

[46] S. Pearson, V. Tountopoulos, D. Catteddu, S. Mario, R. Molva, C. Reich, S. Fischer-h, C. Millard, V. Lotz, M. G. Jaatun, and R. Leenes, "Accountability for Cloud and Other Future Internet Services," in *CloudCom*, 2012, pp. 629–632.

[47] D. Catteddu, M. Felici, G. Hogben, A. Holcroft, E. Kosta, R. Leened, C. Millard, M. Niezen, D. Nunez, N. Papanikolaou, S. Pearson, D. Pradelles, C. Reed, C. Rong, J.-C. Royer, D. Stefanatou, and T. W. Wlodarczyk, "Towards a Model of Accountability for Cloud Computing Services," in *Int. Wkshp. on Trustworthiness, Accountability and Forensics in the Cloud (TAFC)*, 2013, pp. 21–30.

[48] M. Theoharidou, N. Papanikolaou, S. Pearson, and D. Gritzalis, "Privacy Risk , Security , Accountability in the Cloud," in *IEEE Int. Conf. on Cloud Comp. Tech. and Science Privacy*, 2013, pp. 177–184.

[49] W. Hon, E. Kosta, C. Millard, and D. Stefanatou, "Cloud Accountability: The Likely Impact of the Proposed EU Data Protection Regulation," *Qun. Mary Sch. of Law Legal Studies Res. Ppr.*, no. 172, pp. 1–54, 2014.

[50] K. Bernsmed, W. K. Hon, and C. Millard, "Deploying Medical Sensor Networks in the Cloud Accountability Obligations from a European Perspective," in *Cloud Computing (CLOUD), 2014 IEEE 7th International Conference on*. IEEE Comput. Soc, 2014, pp. 898–905.

[51] R. K. L. Ko, "Data Accountability in Cloud Systems," in *Security, Privacy and Trust in Cloud Systems*. Springer, 2014, pp. 211–238.

[52] W. Benghabrit, H. Grall, J.-C. Royer, M. Sellami, M. Azraoui, K. Elkhiyaoui, M. Onen, A. S. D. Olivera, and K. Bernsmed, "A Cloud Accountability Policy Representation Framework," in *CLOSER-4th Int. Conf. on Cloud Comp. and Serv. Science*, 2014, pp. 489–498.

[53] V. Tountopoulos, M. Felici, and A. Pannetrat, "Interoperability Analysis of Accountable Data Governance in the Cloud," in *Cyber Security and Privacy*. Springer International Publishing, 2014, vol. 1, pp. 77–88.

[54] N. Papanikolaou, R. Thomas, and C. Reich, "A Simulation Framework to Model Accountability Controls for Cloud Computing," *CLOUD COMPUTING 2014, The Fifth International Conference on Cloud Computing, GRIDs, and Virtualization*, no. c, pp. 12–19, 2014.

[55] B. Duncan, D. J. Pym, and M. Whittington, "Developing a Conceptual Framework for Cloud Security Assurance," in *Cloud Computing Technology and Science (CloudCom), 2013 IEEE 5th International Conference on (Volume 2)*. Bristol: IEEE, 2013, pp. 120–125.

[56] B. Duncan and M. Whittington, "Company Management Approaches Stewardship or Agency: Which Promotes Better Security in Cloud Ecosystems?" in *CloudCom2015*. Nice: IEEE, 2015, pp. 1–6.

[57] European Commission, "Unleashing the Potential of Cloud Computing in Europe," 2012.

[58] European Commission, "Cloud Service Level Agreement Standardisation Guidelines," EU Commission, Brussels, Tech. Rep., 2014.