Enhancing Cloud Security and Privacy: The Power and the Weakness of the Audit Trail

Bob Duncan
Computer Science
University of Aberdeen
Aberdeen, UK
Email: bobduncan@abdn.ac.uk

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

***Abstract*—Information security in the cloud presents a serious challenge. We have identified fundamental weaknesses when undertaking cloud audit, namely the misconceptions surrounding the purpose of audit, what comprises a proper audit trail, what should be included, and how it should be achieved and maintained. A properly specified audit trail can provide a powerful tool in the armoury against cyber-crime, yet it is all too easy to throw away the benefits offered by this simple tool through lack of understanding, incompetence, mis-configuration or sheer laziness. Of course, merely having an effective audit trail is not enough — we actually have to examine it regularly to realise the potential benefits it offers.**

***Keywords*—security; privacy; audit; audit trail.**

I. Introduction

Achieving information security is not a trivial process. When this involves a cloud setting, the problem intensifies exponentially. Let us first consider how we go about achieving security. Usually, it is achieved by means of compliance with standards, assurance or audit. We provide some useful background on this in [1]. In a non-cloud setting, we have a range of established standards which are well understood by industry. However, when we move to cloud, everything changes. There are an extensive range of cloud standard setting bodies, yet there remains no definitive cloud security standard.

Assurance in non-cloud settings is well understood, but assurance in a cloud setting is less well understood. There are many challenges to overcome and, with Pym, we addressed some of those in earlier work [2] developing a conceptual framework for cloud security assurance, where we addressed: standards, proposed management method and complexity.

One of the fundamental tools that can be used to help ensure cloud security is the simple audit trail. There are, of course, many other challenges, and we revisit these in Section II, where we look at the definition of security goals, compliance with cloud security standards, audit issues, the impact of management approaches on security, and how complexity, the lack of responsibility and accountability affect cloud security. The remainder of the paper is organized as follows: in Section III, we discuss cloud audit, state of the art; in Section IV, we consider misconceptions prevalent across different disciplines of what exactly the audit trail is; in Section V, we discuss how we might improve audit trails in a cloud setting. In Section VI, we discuss our conclusions.

II. Cloud Security Challenges

A number of challenges 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 in an environment using agency theory to manage director self-interest and inter-corporate transactions. Agency theory recognizes the need to align the objective of agent with principal, though this has been shown to be difficult to achieve in practice. Cloud security is no different, which suggests a different approach is needed.

Ten key security issues have been identified, namely:

- The definition of security goals;
- Compliance with standards;
- Audit issues;
- Management approach;
- Technical complexity of cloud;
- Lack of responsibility and accountability;
- Measurement and monitoring;
- Management attitude to security;
- Security culture in the company;
- The threat environment.

Looking at the definition of security goals, we recognise that the business environment is constantly changing, as are corporate governance rules and this would clearly imply changing security measures are required to keep up to date. More emphasis is now placed on responsibility and accountability [3], social conscience [4], sustainability [5] [6], resilience [7] and ethics [8]. Responsibility and accountability are, in effect, mechanisms we can use to help achieve all the other security goals. As social conscience and ethics are very closely related, we can expand the traditional CIA triad to include sustainability, resilience and ethics. This expansion of CIA can help address some of the shortcomings of agency theory, but also provides a perfect fit to stewardship theory. Stewardship carries a broader acceptance of responsibility than the self-interest embedded in agency, extending to acting in the interests of company owners, society and the environment as a whole. Broadening the definition of security goals gives a more effective way to achieve successful cloud audit, but the added complexity cloud brings may complicate the audit trail.

In earlier work with Pym [2], we developed a conceptual framework to address cloud security. We identified three barriers to good cloud security: standards compliance, management method and complexity. We addressed compliance with standards in [1]. The lack of coherent cloud standards undermines the effectiveness of cloud audit and highlights a fundamental weakness in that process [9] — the use of checklists.

We also considered management method [10], where we addressed the cloud security issue with management method, arguing that historic reliance on agency theory to run companies can undermine effective security. We addressed complexity along with the difficulties in addressing measurement [11],

 ISBN: 978-1-61208-460-2

which can complicate effective audit. In [12], we addressed the lack of responsibility and accountability in standard service level agreements (SLAs). This area has been much neglected, but there are signs that it is being taken more seriously.

On the matter of achieving compliance with standards 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, a number of cloud security standards have evolved, but the problem is that there is still no standard which offers 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 [1]. The pace of evolution of new technology far outstrips the capability of international standards organisations to keep up with the changes [13], adding to the problem and meaning it may not be resolved any time soon. We have argued that companies need to take account of these gaps in the standards when addressing compliance. Reliance on compliance alone will undermine effective security. Some key areas above we will not address here. Management attitude to security, the importance of developing a strong security culture in the company, and looking at the threat environment are all areas that merit more extensive and specific research.

We have also considered weaknesses in the approach to cloud audit [14], and we expand on that work here. It is certainly the case that cloud audit is not a mature field, and much early work on cloud audit has focussed on addressing technical issues. We have long held the view that focussing on technical issues alone can never solve cloud security. The business architecture of a company comprises people, process and technology [15], not technology alone, thus focussing on a technical solution alone is likely to undermine security.

III. Cloud Audit, the State of the Art

Vouk [16], in an early description of cloud computing issues, suggests there must be an ability to audit processes, data and processing results, but does not propose a solution. Wang et al. [17] address how the cloud paradigm brings about many new security challenges, which have not been well understood. The authors study the problem of ensuring the integrity of data storage in cloud computing, in particular, the task of allowing a third party auditor (TPA), working on behalf of the cloud client, to verify the integrity of the dynamic data stored in the cloud. The authors identify the difficulties, potential security problems and show how to construct an elegant verification scheme for seamless integration of these features into protocol design, but this relies on the willingness of the cloud service provider (CSP) to permit the TPA entry to their systems.

Leavitt [18] suggests CSPs will not be able to pass customer audits if they cannot demonstrate who has access to their data and how they prevent unauthorised personnel from retrieving information. Again, there is no detail given on how to address this. Some CSPs address this by appointing TPAs to audit their systems in advance, and by documenting procedures designed to address customers' data security needs. Bernstein et al. [19] are excited by the prospect of a "cloud of clouds", but are worried about the security processes used to ensure connectivity to the correct server on the other clouds, suggesting some kind of audit-ability would be needed. The authors stress the need for cloud systems to provide strong and secure audit trails, but do not suggest how this might be done.

Pearson and Benameur [20] recognise that achieving proper audit trails in the cloud is an unresolved issue. Wang et al. [21] address privacy preserving public auditing for data storage security in cloud, and are keen to prevent TPA introduced weaknesses to the system, presenting a mechanism to enable a more secure approach to public audit by TPAs. Development of the algorithms is at an early stage and the authors note further improvement needs to take place. Zhou et al. [22] carry out a survey on security and privacy in cloud computing, investigating several CSPs about their concerns on security and privacy issues, and find those concerns are inadequate. The authors suggest more should be added in terms of five aspects (i.e., availability, confidentiality, data integrity, control and audit) for security, but do not provide any detail. Chen and Yoon [23] present a framework for secure cloud computing through IT auditing by establishing a general framework using checklists by following data flow and its life-cycle. The checklists are made based on the cloud deployment models and cloud services models, see [9] for our views on checklists.

Armbrust et al. [24] present a detailed description of what cloud computing is, and note that the possible lack of auditability presents the number three barrier to implementation, without proposing any solution. Ramgovind et al. [25] provide an overall security perspective of cloud computing with the aim of highlighting the security concerns that should properly be addressed and managed to realise the full potential of cloud computing. The authors note that possible unwillingness of CSPs to undergo audit presents a real barrier to acceptance and take up. Grobauer et al. [26] note that discussions about cloud computing security often fail to distinguish general issues from cloud-specific issues. The authors express concern that many CSPs do not do enough to ensure the provision of good cloud audit practice and hence evidence proper security.

Doelitzscher et al. [27] present a prototype demonstration of Security Audit as a Service (SAaaS) architecture, a cloud audit system which aims to increase trust in cloud infrastructures by introducing more transparency to both user and cloud provider on what is happening in the cloud. This system aims to keep track of changes to the infrastructure as VMs are deployed, moved or shut down. Hale and Gamble [28] note that current SLAs focus on quality of service metrics and lack the semantics needed to express security constraints that could be used to measure risk. The authors present a framework, called SecAgreement (SecAg), that extends the current SLA negotiation standard to allow security metrics to be expressed on service description terms and service level objectives. The framework seeks to provide a lightweight approach, which can leave some weaknesses not fully addressed.

Pappas et al. [29] present CloudFence, a framework that allows users to independently audit the treatment of their private data by third-party online services, through the intervention of the cloud provider that hosts these services. The authors demonstrate that CloudFence requires just a few changes to existing application code, while it can detect and prevent a wide range of security breaches, ranging from data leakage attacks using SQL injection, to personal data disclosure due to missing or erroneously implemented access control checks. It addresses data held by a CSP, but does not claim to provide a complete audit trail. Xie and Gamble [30] outline a tiered

 ISBN: 978-1-61208-460-2

approach to auditing information in the cloud, but with little detail provided. The approach provides perspectives on auditable events that may include compositions of independently formed audit trails. Zhu et al. [30] propose the use of provable data possession (PDP), a cryptographic technique for verifying the integrity of data, without retrieving it, as part of a means of carrying out audit on the data. This tool can prove the integrity of data, but does not consider who has accessed the data.

Ruebsamen and Reich [31] propose the use of software agents to carry out continuous audit processing and reporting. The authors propose continuous audit to address the dynamically changing nature of cloud use, so as to ensure evidence concerning vital periods of use are not missed. The use of a separate evidence store is a major plus, and the tools developed look very interesting. The authors note that an audit of the cloud layer alone will not be enough. Doelitzscher et al. [32] propose the use of neural networks to analyse and learn the normal usage behaviour of cloud customers, so that anomalies which originate from a cloud security incident caused by a compromised virtual machine can be detected. While retrospective tests on collected data have proved very effective, the system has yet to reach a sufficient level of maturity to be deployed in a live environment.

Doelitzscher et al. [33] present a cloud audit policy language for their SAaaS architecture. The authors describe the design and implementation of the automated audit system of virtual machine images, which ensures legal and company policies are complied with. They also discuss how on-demand software audit agents that maintain and validate the security compliance of running cloud services are deployed. Thorpe et al. [34] present a framework for forensic based auditing of cloud logs. The authors explore the requirements of a cloud log forensics service oriented architecture (SOA) framework for performing effective digital investigation examinations in these abstract web services environments. Of course, these services need to be activated and protected before these tools can be deployed. Wang et al. [35] propose a secure cloud storage system supporting privacy-preserving public auditing. The authors further extend their proposal to enable the TPA to perform audits for multiple users simultaneously and efficiently, an improvement on earlier work.

Lopez et al. [36] propose privacy-friendly cloud audits by applying Somewhat Homomorphic Encryption (SHE) and Public-Key Searchable Encryption (PEKS) to the collection of digital evidence. The authors show that their solution can provide client privacy preserving audit data to cloud auditors. Whilst good for privacy, this does not cover all angles. Shameli-Sendi and Cheriet [37] propose a framework for assessing the security risks associated with cloud computing platforms, but propose no solution on how to achieve a high standard of audit. Xiong and Chen [38] consider how to allocate sufficient computing resources, but not to over-provision them, to process and analyse audit logs for ensuring the guarantee of security of an SLA, referred to as the SLA-based resource allocation problem, for high-performance cloud auditing. This is interesting because of the tools developed. However, it is geared toward enforcement of SLAs in high performance computing, rather than for security auditing.

The common theme running through much of this work is that there is a recognition of the need for proper audit, but little idea of how to go about it. Where tools are developed, many are excellent for what they are designed for, but do not offer a complete solution to the problem. It is clear that the consistent lack of input from the accounting profession is not helping advance the state of the art, and we would call for more input from the accounting profession. Cloud computing is such a radical change from traditional computing approaches, that we now need to involve a wider range of disciplines, working together to try to address what represents a major challenge.

IV. The Audit Trail

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 [1] provide some background on this issue. Cloud computing audit can not be considered a mature field, and there will be some way to go before it can catch up with the reflection and rigour of 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.

A fundamental element of the audit process is the audit trail, and having two disciplines involved in providing cloud audit services means we have two different disciplines to contend with, namely accounting professionals and security professionals. An obvious concern is what is meant by the term "audit trail". It is easy to assume that everyone is talking about the same thing, but is that actually the case? To an accounting professional, the meaning of an audit trail is very clear.

The Oxford English Dictionary (OED) [39] has two useful definitions of an audit trail: "(a) Accounting: a means of verifying the detailed transactions underlying any item in an accounting record; (b) Computing: a record of the computing processes which have been applied to a particular set of source data, showing each stage of processing and allowing the original data to be reconstituted; a record of the transactions to which a database or a file has been subjected". This suggests common understanding, but often this is not evident in computing research.

Some 20 years ago, the National Institute of Standards and Technology (NIST) [40] provided, in the context of computing security, a very detailed description of what an audit trail is, and this is wholly consistent with the OED definition. When we look at the definitions in use in some cloud audit research papers, we start to see a less rigorous understanding of what an audit trail is. For example, Bernstein [19] suggests the audit trail comprises: events, logs, and analysis thereof, Chaula [41] suggests: raw data, analysis notes, preliminary development and analysis information, processes notes, etc.

Pearson et al. [20] recognise that achieving proper audit trails in the cloud is an unresolved issue. Ko et al. [42] explicitly note that steps need to be taken to prevent audit trails disappearing after a cloud instance is shut down. Ko [43] recognises the need to collect a multiplicity of layers of log data, including transactional audit trails in order to ensure accountability in the cloud. The EU Article 29 Working Party [44] raises several cloud-specific security risks, such as loss of governance, insecure or incomplete data deletion, insufficient

 ISBN: 978-1-61208-460-2

audit trails or isolation failures, which are not sufficiently addressed by existing Safe Harbor principles on data security.

The audit trail can be a very powerful tool in the fight against attack. Just as the audit trail offers forensic accountants a means to track down fraudulent behaviour in a company, so the audit trail in a cloud setting, providing it can be properly protected against attack, offers forensic scientists an excellent basis to track intrusions and other wrongdoing. In the event of a catastrophic attack, it should be possible to reconstruct the system that has been attacked, in order to either prove the integrity of the system values, or in a worst case scenario, reconstruct the system from scratch. The redundancy offered by the simple audit trail, often seen by many as an unnecessary duplication, will prove invaluable in the event of compromise.

Many cloud users are punctilious about setting up proper audit trails, but sometimes forget that when a virtual machine (VM) running in the cloud is shut down, everything, including the audit trail data they have so assiduously collected, disappears as soon as the VM shuts down [42], unless steps are taken to prevent this loss. In real world conditions, most database software ships with inadequate audit trail provision in the default settings. Anderson [45] states that the audit trail should only be capable of being read by users. While it is simple enough to restrict users to read-only access, this does not apply to the system administrators. This presents an issue where an intruder gets into a system, escalates privileges until root access is obtained, and is then free to manipulate, or delete the audit trail entries in order to cover their tracks.

Cloud users often assume that the VMs they are running will be under their sole control. However, the VMs run on someone else's hardware — the CSP's, who also employ system administrators, and sometimes employ temporary staff, some of whom are also system administrators. While the CSP may vet their own staff to a high level, this is often overlooked with temporary employees. Network connections too are often virtualised, opening up yet more avenues of attack.

A cloud user can take as many steps to secure their business as they wish, but a key ingredient in the equation is the fact that all cloud processes run on somebody else's hardware, and often software too — the CSP's. The cloud relationship needs to include the CSP as a key partner in the pursuit of achieving security [12]. Unless and until CSPs are willing to share this goal, technical solutions will be doomed to failure.

V. How can we improve the audit trail?

These vulnerabilities are not new, and are well known to security professionals, and while many companies do use security professionals, many do not. Regardless, companies continue to be breached. As stated in the introduction, achieving information security is not a trivial process, but in a cloud setting, this becomes far more difficult, due to the complexity of relationships between myriad actors involved in cloud ecosystems, as well as the other issues discussed in Section II. Audit is difficult. Cloud audit is far more difficult, with far more weaknesses to overcome. Proper audit trails alone will not solve cloud security, but will go a long way to helping with this goal if some simple steps are taken.

In the accounting world, an understanding of exactly what is meant by an audit trail, and its importance, is a fundamental part of the training every accountant undertakes. Looking at the literature on cloud audit, it is obvious that there is a need for input from the accounting profession, and the authors would wish to encourage and see more input from that source. It is clear that there is no shortage of input on the technical side, but the authors believe there is room for a valuable contribution to be made by the accounting profession, with many lessons learned over many decades. There is also no doubt that further work is needed, and work on audit trails can prove to be both cost effective and productive in helping with security.

Some interesting work is being done on information flow control and legal issues in cloud [46] [47] [48] [49] [50] [51] which we believe, while a little light on the audit side, has the potential to offer good improvements to cloud users to enhance their security and privacy, and to achieve compliance.

In looking at the current approach to the use of the audit trail, there are three fundamental weaknesses which need to be addressed, yet which are relatively simple to address. First, inadequate default logging options can result in insufficient data being collected for the audit trail. Second, there is a lack of recognition that the audit trail data can be accessed by a malicious user gaining root privileges, which can lead to the removal of key data showing who compromised the system, and what they did once they had control of it. Third, failure to ensure log data is properly collected and moved to permanent storage can lead to loss of audit trail data, either when an instance is shut down, or when it is compromised. These weaknesses apply equally to cloud and non-cloud systems.

On the first point, we look at one of the most popular open source database programmes in general use today — MySQL. The vast majority of implementations use standard default settings on installation, or install the programme as part of a standard Linux, Apache, MySQL and PHP (LAMP) server. With a LAMP server, all four of the constituent elements are set up using the default settings. This works very well for easy functionality "out of the box", which is the aim of a LAMP server. But, this does not adequately address security in the four elements of the LAMP server, and applies equally to cloud and non-cloud systems.

MySQL offers the following audit trail options:

- Error log — Problems encountered starting, running, or stopping mysqld;
- General query log — Established client connections and statements received from clients;
- Binary log — Statements that change data (also used for replication);
- Relay log — Data changes received from a replication master server;
- Slow query log — Queries that took more than long_query_time seconds to execute;
- DDL log (metadata log) — Metadata operations performed by Data Definition Language (DDL) statements.

By default, no logs are enabled, except the error log on Windows. Some versions of Linux send the Error log to syslog.

Oracle offer an audit plugin for Enterprise (paid) Editions of MySQL. This allows a range of events to be logged, but again, by default, most are not enabled. The MariaDB company, whose author originally wrote MySQL, have their own open source audit plug-in, and offer a version suitable for MySQL. It has the following functionality:

 ISBN: 978-1-61208-460-2

- CONNECTION — Logs connects, disconnects and failed connects (including the error code);
- QUERY — Queries issued and their results (in plain text), including failed queries due to syntax or permission errors;
- TABLE — Which tables were affected by query execution;
- QUERY_DDL — Works as the 'QUERY' value, but filters only DDL-type queries (CREATE, ALTER, etc);
- QUERY_DML — Works as the 'QUERY' value, but filters only Data Manipulation Language (DML) DML-type queries (INSERT, UPDATE, etc).

By default, logging is set to off. Thus, those users who rely on default settings for their systems are immediately putting themselves at a severe disadvantage.

On the second point, as Anderson [45] states, the audit trail should only be capable of being read by users. This presents a problem in a cloud setting, where the software being used is running on someone else's hardware. There is a risk of compromise from an outside user with malicious intent. There is also a risk of compromise by someone working for the CSP. While the CSP may well take vetting of staff seriously, there may be situations that arise where a temporary contract worker is engaged at short notice who is subject to lesser scrutiny. This applies equally to cloud and non-cloud systems.

Looking at the third point, where MySQL data logging is actually switched on, all data is logged to the running instance. This means the data remains accessible to any intruder who successfully breaches the system, allowing them to cover their own tracks by deleting any entries which relate to their intrusion of the system, or to simply delete the entire audit trail files. And, when the running instance is shut down, all the data disappears anyway. In a non-cloud situation, the data is still visible to the attacker, but the forensic trail may still be left for investigation. However, in a cloud instance, if the data is not safely stored and the running instance is shut down, the forensic trail is more likely to be permanently lost.

These three points are not generally considered, yet they present a serious weakness to the success of maintaining the audit trail. Yet, these are relatively trivial to address by simply turning on data logging and sending all log output to an independent secure server under the control of the cloud user. Adding an Intrusion Detection system (IDS) is also a useful additional precaution to take, and this should be run on an independent secure server under the control of the cloud user. Using an audit plug-in in addition to all the basic logging capabilities, is also a useful thing to do. While there may be some double processing involved, it is better to have more data than none at all. Where the MySQL instance forms part of a LAMP server, it would be prudent to make some elementary security changes to the setup of the Linux operating system, the Apache web server, and to harden the PHP installation.

It is rather worrying that in 2012, [52] report an average of 6 months between breach and discovery, a clear indication that very few firms scrutinise their server logs, with most discovery being advised by external bodies, such as customers, financial institutions or fraud agencies. It is encouraging to see that three years later [53], the time between breach to discovery has been drastically reduced. This still leaves a large gap where compromised systems may still be under the control of malicious users, which is a worry. Thus, in addition to making the simple suggestions we propose above, cloud users should also make sure they actually review their audit trail logs. It is vital to understand when a security breach has occurred, which records have been accessed, compromised or stolen. While this is not a foolproof method of achieving cloud security, it is an effective first step to help deliver far higher affordable security than many companies currently achieve.

The authors have over 50 years of experience of audit and internal audit in industry between them, and this knowledge has been brought to bear in addressing this work. This initial review of the state of the art raises serious concerns over how little is being done. With some input from and partnership with the accounting profession, it may be possible to work to achieve far more effective levels of cloud audit, which in turn, can lead to better levels of security being achieved.

VI. Conclusion

We have looked at some of the challenges facing companies who seek to obtain good cloud security assurance. We have seen how weaknesses in standard CSP SLAs can impact on cloud security. We have identified cloud security standards issues, and how that might impact cloud security. We have considered how the lack of accountability can impact security. We have discussed how these issues must also be addressed.

The practice of using default settings when installing software in a cloud environment is clearly asking for trouble, yet still persists. The simple steps proposed by the authors are relatively easy to implement, need not be particularly expensive to implement and maintain, and providing some on-going monitoring of the audit trail logs is carried out, will certainly prove beneficial. Inspecting the logs need not be challenging or costly — there are many software solutions available to address this task. Complicated solutions generally lead to complex problems, as the more complex the solution, the more the risk of ineffective configuration and maintenance can lead to compromise in security. Yet all too often, the simple steps that can really help improve security are ignored.

We certainly believe that more work needs to be done in this area, and it would be beneficial to encourage the accounting audit profession to get involved. After all, it is their neck on the block when they sign off an audit, and anything that can reduce risk to themselves, as well as their clients, has to be a good thing. We have touched on how these difficult areas of security might easily be approached as part of a comprehensive security solution using simple and inexpensive methods. Clearly, companies could benefit from further research in several of these areas. It is also clear that no one profession is equipped to deal with this challenge. However, we would caution that action is needed now, not several years down the line when research reaches a more complete level of success in these areas. The threat environment is too dangerous. Companies have to act now to try to close the door, otherwise it may be too late.

References

[1] B. Duncan and M. Whittington, "Compliance with Standards, Assurance and Audit: Does this Equal Security?" in Proc. 7th Int. Conf. Secur. Inf. Networks. Glasgow: ACM, 2014, pp. 77–84.

 ISBN: 978-1-61208-460-2

[2] B. Duncan, D. J. Pym, and M. Whittington, "Developing a Conceptual Framework for Cloud Security Assurance," in Cloud Comp. Tech. Sci. (CloudCom), 2013 IEEE 5th Int. Conf. (Vol. 2). Bristol: IEEE, 2013, pp. 120–125.

[3] M. Huse, "Accountability and Creating Accountability: a Framework for Exploring Behavioural Perspectives of Corporate Governance," Br. J. Manag., vol. 16, no. S1, 2005, pp. S65–S79.

[4] A. Gill, "Corporate Governance as Social Responsibility: A Research Agenda," Berkeley J. Int'l L., vol. 26, no. 2, 2008, pp. 452–478.

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

[6] A. Kolk, "Sustainability, accountability and corporate governance: Exploring multinationals' reporting practices." Bus. Strateg. Environ., vol. 17, no. 1, 2008, pp. 1–15.

[7] F. S. Chapin, G. P. Kofinas, and C. Folke, Principles of ecosystem stewardship: Resilience-based natural resource management in a changing world. Springer, 2009.

[8] S. Arjoon, "Corporate Governance: An Ethical Perspective," J. Bus. Ethics, vol. 61, no. 4, 2012, pp. 343–352.

[9] B. Duncan and M. Whittington, "Reflecting on Whether Checklists Can Tick the Box for Cloud Security." in Cloud Comp. Tech. Sci. (CloudCom), IEEE 6th Int. Conf., Singapore: IEEE, 2014, pp. 805–810.

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

[11] B. Duncan and M. Whittington, "The Importance of Proper Measurement for a Cloud Security Assurance Model," in Cloud Comp. Tech. Sci. (CloudCom), 2015 IEEE 7th Int. Conf., Vancouver, 2015, pp. 1–6.

[12] B. Duncan and M. Whittington, "Enhancing Cloud Security and Privacy: Broadening the Service Level Agreement," in Trustcom/BigDataSE/ISPA, IEEE. Vol. 1. IEEE, Helsinki, 2015, pp. 1–6.

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

[14] B. Duncan and M. Whittington, "Enhancing Cloud Security and Privacy: The Cloud Audit Problem," in press.

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

[16] M. Vouk, "Cloud computing- Issues, research and implementations," ITI 2008 - 30th Int. Conf. Inf. Technol. Interfaces, vol. 16, no. 4, 2008, pp. 235–246.

[17] L. Wang, J. Zhan, W. Shi, Y. Liang, and L. Yuan, "In cloud, do MTC or HTC service providers benefit from the economies of scale?" Proc. 2nd Work. Many-Task Comp. Grids Supcomp. - MTAGS, 2009, pp. 1–10.

[18] N. Leavitt, "Is Cloud Computing Really Ready for Prime Time?" Computer (Long. Beach. Calif)., vol. 42, no. January, 2009, pp. 15–20.

[19] D. Bernstein, E. Ludvigson, K. Sankar, S. Diamond, and M. Morrow, "Blueprint for the intercloud - Protocols and formats for cloud computing interoperability," in Proc. 2009 4th Int. Conf. Internet Web Appl. Serv. ICIW 2009, 2009, pp. 328–336.

[20] S. Pearson and A. Benameur, "Privacy, Security and Trust Issues Arising from Cloud Computing," 2010 IEEE Second Int. Conf. Cloud Comput. Technol. Sci., 2010, pp. 693–702.

[21] C. Wang, S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage in Cloud Computing," in IEEE Trans. Comput., vol. PP, no. 99, 2012, pp. 1–14.

[22] M. Zhou, R. Zhang, W. Xie, W. Qian, and A. Zhou, "Security and Privacy in Cloud Computing: A Survey," in 2010 Sixth Int. Conf. Semant. Knowl. Grids, 2010, pp. 105–112.

[23] Z. Chen and J. Yoon, "IT Auditing to Assure a Secure Cloud Computing," in 2010 6th World Congr. Serv., 2010, pp. 253–259.

[24] M. Armbrust et al., "A view of cloud computing," Commun. ACM, vol. 53, no. 4, 2010 pp. 50–58.

[25] S. Ramgovind, M. M. Eloff, and E. Smith, "The management of security in cloud computing," in Proc. Inf. Sec. S. A. Conf. ISSA, 2010, pp. 1–7.

[26] B. Grobauer, T. Walloschek, and E. Stöcker, "Understanding cloud computing vulnerabilities," IEEE Secur. Priv., vol. 9, no. 2, 2011, pp. 50–57.

[27] F. Doelitzscher et al., "Validating cloud infrastructure changes by cloud audits," in Proc. - 2012 IEEE 8th World Congr. Serv. Serv. 2012, 2012, pp. 377–384.

[28] M. L. Hale and R. Gamble, "SecAgreement: Advancing security risk calculations in cloud services," in Proc. - 2012 IEEE 8th World Congr. Serv., 2012, pp. 133–140.

[29] V. Pappas, V. Kemerlis, A. Zavou, M. Polychronakis, and A. D. Keromytis, "CloudFence: Enabling Users to Audit the Use of their Cloud-Resident Data," 2012.

[30] Y. Zhu, H. Hu, G.-J. Ahn, and S. S. Yau, "Efficient audit service outsourcing for data integrity in clouds," J. Syst. Softw., vol. 85, no. 5, 2012, pp. 1083–1095.

[31] T. Ruebsamen and C. Reich, "Supporting cloud accountability by collecting evidence using audit agents," in Proc. Int. Conf. Cloud Comput. Technol. Sci. CloudCom, vol. 1, 2013, pp. 185–190.

[32] F. Doelitzscher, M. Knahl, C. Reich, and N. Clarke, "Anomaly Detection In IaaS Clouds," in CloudCom, 2013, pp. 387–394.

[33] F. Doelitzscher et al., "[DRKK+13] Sun Behind Clouds - On Automatic Cloud Security Audits and a Cloud Audit Policy Language," J. Adv. vol. 6, no. 1, 2013, pp. 1–16.

[34] S. Thorpe et al., "Towards a forensic-based service oriented architecture framework for auditing of cloud logs," in Proc. - 2013 IEEE 9th World Congr. Serv. Serv. 2013, 2013, pp. 75–83.

[35] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for secure cloud storage," IEEE Trans. Comput., vol. 62, no. 2, 2013, pp. 362–375.

[36] J. M. López, T. Ruebsamen, and D. Westhoff, "Privacy-Friendly Cloud Audits with Somewhat Homomorphic and Searchable Encryption," in Innov. Com. Serv. (I4CS), 14th Int. Conf., 2014, pp. 95–103.

[37] A. Shameli-Sendi and M. Cheriet, "Cloud Computing: A Risk Assessment Model," Cloud Eng. (IC2E), IEEE Int. Conf., 2014, pp. 147–152.

[38] K. Xiong and X. Chen, "Ensuring Cloud Service Guarantees Via Service Level Agreement (SLA) -based Resource Allocation," in Dist. Comp. Sys. Work. (ICDCSW), IEEE 35th Int. Conf., 2015, pp. 35–41.

[39] OED, "Oxford English Dictionary," 1989. [Online]. Available: www.oed.com [Retrieved: Feb 2016]

[40] D. Gollmann, "Computer Security," NIST, Tech. Rep. 800, 2011.

[41] J. Chaula, "A Socio-Technical Analysis of Information Systems Security Assurance: A Case Study for Effective Assurance," Ph.D. thesis, 2006.

[42] R. K. L. Ko et al., "TrustCloud: A framework for accountability and trust in cloud computing," Proc. - IEEE World Cong. Serv., 2011, pp. 584–588.

[43] L. F. B. Soares, D. A. B. Fernandes, J. V. Gomes, M. M. Freire, and P. R. M. Inácio, "Security, Privacy and Trust in Cloud Systems," in Secur. Priv. Trust Cloud Syst. Springer, 2014, ch. Data Accou, 2014, pp. 3–44.

[44] Eu, "Unleashing the Potential of Cloud Computing in Europe," 2012.

[45] R. J. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, C. A. Long, Ed. Wiley, 2008, vol. 50, no. 5.

[46] T. Pasquier, B. Shand, and J. Bacon, "Information Flow Control for a Medical Records Web Portal," Cl.Cam.Ac.Uk, 2013, pp. 1–8.

[47] J. Bacon et al., "Information flow control for secure cloud computing," IEEE Trans. Netw. Serv. Manag., vol. 11, no. 1, 2014, pp. 76–89.

[48] T. F. J. Pasquier, J. Singh, J. Bacon, and O. Hermant, "Managing Big Data with Information Flow Control," in Cloud Comput. Technol. Sci. (CloudCom), 2015 IEEE 7th Int. Conf., vol. 2, 2015, pp. 1–8.

[49] J. Singh et al., "Regional Clouds: Technical Considerations," no. UCAM-CL-TR-863, 2014.

[50] J. Singh, J. Powles, T. Pasquier, and J. Bacon, "Seeing through the clouds: Management, control and compliance for cloud computing," Cloud Comput., 2015, pp. 1–12.

[51] W. Hon, E. Kosta, C. Millard, and D. Stefanatou, "Cloud Accountability: The Likely Impact of the Proposed EU Data Protection Regulation," Queen Mary Sch. Law Leg. Stud. Res. Pap., no. 172, 2014, pp. 1–54.

[52] Trustwave, "2012 Global Security Report," Tech. Rep., 2012.

[53] Verizon, "Verizon 2015 Data Breach Investigation Report," Tech. Rep., 2015.

 ISBN: 978-1-61208-460-2