Cloud Cyber-Security: Empowering the Audit Trail

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—**Cyber-security presents a serious challenge. Cyber-security in the cloud presents a far more serious challenge, due to the multi-tenant nature of cloud relationships and the transitory nature of cloud instances. We have identified a fundamental weakness 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. A major weakness is the need to ensure the audit trail is properly preserved. We propose that some simple changes in approach are undertaken, which can considerably improve the status quo, while radically improving the ability to conduct forensic examination in the event of a breach, but of course, merely having an effective audit trail is not enough — we actually have to analyse it regularly to realise the potential benefits it offers.**

Keywords—cloud cyber-security; compliance; assurance; audit; audit trail.

I. INTRODUCTION

This article is based on an extended version of our 2016 paper [1], in which we examined the possible strengths and weaknesses of the proper use of the audit trail in cloud cyber security. 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 [2]. 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 no comprehensive cloud security standard yet exists. We outline the status of cloud security standards in Section V.

Often, when a company moves its programmes to a cloud setting, there is an assumption that it is a straight transfer. Assurance in a non-cloud setting is well understood, but assurance in a cloud setting is much less well understood. There are a great many challenges to overcome and we addressed some of those in earlier work [3], with a colleague, developing a conceptual framework for cloud security assurance, where we addressed three key challenges, namely standards compliance, management method and complexity. There are a great many issues to consider, and many common mistakes are made in this process, and we discuss some of the most common of these in Section III.

One of the fundamental, long standing security concepts for internal business control is the concept of separation of duties, which is designed to remove both opportunity and temptation from staff employed in the business, and we look at this in more detail in Section IV.

A further primary tool 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, how the technical complexity of cloud and the lack of responsibility and accountability affects cloud security. We look at the need for, and benefits derived from, proper measurement and monitoring. We also consider the impact of management attitude to security, the security culture in the company and the threat environment, both external and the possible impact of internal threats. In Section III, as noted above, we discuss some of the most common mistakes companies make when adopting cloud computing, and in Section IV, as already mentioned above, we review the separation of duties in more detail. In Section V, we review the current state of cloud security standards. The remainder of the paper is organized as follows: in Section VI we discuss how the literature approaches cloud auditing; in Section VII we consider the misconceptions prevalent across different disciplines of what exactly the audit trail is; in Section VIII we discuss how we might go about improving the audit trail in a cloud setting, suggesting the use of some simple measures that can easily be taken to improve the status quo. In Section IX, we provide a useful reminder of who should be responsible for carrying out mitigating steps for the problem areas, and in Section X we discuss our conclusions.

II. CLOUD SECURITY CHALLENGES

There are a number of challenges that 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 framework developed when it was common practice for corporate management to run a company under agency theory. We have all seen how agency theory has failed to curb the excesses of corporate greed. The same is true when applied to cloud security, which would suggest a different approach is needed.

Ten key security issues have been identified, namely:

- The definition of security goals [6];
- Compliance with standards[3] [2];
- Audit issues [2] [13];
- Management approach [3] [25];

- Technical complexity of cloud [3] [14];
- Lack of responsibility and accountability [6] [14];
- Measurement and monitoring [14];
- Management attitude to security [1];
- Security culture in the company [1];
- The threat environment [25].

These 10 key security issues are not the only issues that need to be tackled, but in our opinion, these represent the issues that present the greatest barriers to achieving a good level of cloud security. We discuss each of these in turn below.

In looking at the definition of security goals, we have recognised that the business environment is constantly changing, as are corporate governance rules and this would clearly imply changing security measures would be required to keep up to date. Many managers are unable, unwilling or unsure of how to define proper security goals [4] [5] [6]. More emphasis is now being placed on responsibility and accountability [7], social conscience [8], sustainability [9][10], resilience [11] and ethics [12]. 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, we can expand the traditional CIA triad to include sustainability, resilience and ethics (SRE). This expansion of security requirements can help address some of the short-comings 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. This breadth extends to acting in the interests of company owners and potentially society and the environment as a whole. Broadening the definition of security goals provides a more effective means of achieving a successful cloud audit, although the additional complexity cloud brings will potentially complicate the audit trail.

In earlier work [3], we developed a conceptual framework to address cloud security. In this work, we identified three key barriers to good cloud security, namely standards compliance, management method and complexity. We have already addressed compliance with standards [2]. The lack of coherent cloud standards undermines the effectiveness of cloud audit as well as introducing a fundamental weakness in that process [13] — the use of checklists. We also addressed complexity as part of [14]. Naturally, there are not just three barriers to good security to contend with, as we see from the above list.

On the matter of achieving compliance with cloud security 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 that 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 [2]. The pace of evolution of new technology far outstrips the capacity of international standards organisations to keep up with the changes [15], 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 issues of compliance. Reliance on compliance alone will undermine effective security. We believe that standards need to shift from a rule based approach to a risk based approach [16] [17] [18] [19] [5] [20].

In [21], we addressed the basic issues faced in cloud audit, namely the misunderstandings prevalent concerning the reasons for audit, where we identified the three main purposes of audit. We considered the impact of many factors on the audit process, including addressing the impact of these shortcomings on the successful outcome of the process. 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 [22], not technology alone, thus focussing only on a technical solution is likely to undermine security. We suggest that management need to better understand the purpose, and importance, of audit [21] [23] [6] [14] [24]. It is also necessary to understand both the key importance and weaknesses offered by the audit trail [1].

We also considered the management approach [25], where we addressed the cloud security issue with management method, and argued that the historic reliance on agency theory to run companies can undermine effective security, and we outlined what the impact of this might be on security. There is no doubt that management approach is a key consideration to be aware of in addressing the complex relationships in the cloud ecosystem [25]. While all actors do not utilise the same approach, it is certainly helpful for management to recognise the management approach used by each of the actors involved within their own cloud ecosystem. This will better arm them to identify key risks they face and take appropriate mitigating action.

Having started to address complexity of cloud in [14], it is clear that there is a need for further research in this area. Too many cloud users take the view that cloud is a simple paradigm to use, but are unaware of the serious impact presented by the complexities of cloud. The increasing complexity that new technology brings, results in increased potential exposure to risk as a result of failure to grasp the significance of these risks [26]. Traditional distributed information systems present a multiplicity of technical layers, each of which must interact with one or more other layers, and this is already well understood. Cloud introduces further layers, each of which can be operated by different actors. Cloud brokers may also be involved, leading to yet more layers, more complexity, and more risk. This is an area that is less well understood. Cloud allows a user to quickly deploy, for example, a web server with a database back end, often relying on default settings, which can introduce a number of weaknesses [21]. These default settings usually pay far more attention to usability than to security.

Monahan and Yearworth [27] observe that Service Level Agreements (SLAs) should be meaningful, both for cloud users and providers, as defined by some objective criteria. 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. Duncan and Whittington [6] provide some useful background on these issues in SLAs. It is hard to allocate proper responsibility to the right actors [28], personal data [29] and privacy [30], far less persuade them to accept responsibility for it. Some [31] [30] [32], have long argued that responsibility and accountability should always be built in to the design of cloud systems.

While there has already been extensive research conducted into the security concepts of CIA, there is less research into our additional goals of SRE, We do see a good deal of research into measurement of Corporate Social Responsibility (CSR), [33] [34] [35] [36] [37] [38] [39] [40], resilience [41] [42] [43] [44] [45] [46] [47] [48] and sustainability [49] [50] [51], yet there is still some way to go before effective measures are properly developed and deployed. While measurement is extremely important, it can be very difficult to achieve. There is a clear need to use continuous monitoring when it comes to security management. Reports from global security companies, which cover both non-cloud and cloud data [22], [52], [53], suggest that over 85% of security breaches are achieved with a low level of technical competence, often facilitated by lack of understanding, lack of competence, or poor configuration of victims' systems. Duncan and Whittington [14] provide some useful background on this.

Our first key goal was to define proper security goals, and obviously proper measurement is essential to be able to understand whether these goals can be met. This obviously requires constant monitoring to ensure the goals are actually achieved, or to warn of possible failures before it becomes a more serious problem.

Management attitude to security has been a high priority [54] for a considerable time. In [55], 77% of security professionals have recognised the need to set security attitudes from the top. According to a report [22], management attitude is high, if you listen to the executives, yet low when you listen to IT practitioners. Thus management need to be fully aware that it is not simply a technical issue to be passed down the line, rather it is a fundamental business process that needs to be driven right from the top of the organisation. Information security presents one of the largest risks facing business today and needs to be given the proper attention and commitment it requires.

One of the most important aspects of creating good security in a company lies in the development and maintenance of a good security culture within the organisation. This has long been recognised [54] [55] [22], but its success is dependant on the attitude to security displayed by top management. This attitude must be coupled with proper staff training to ensure staff understand how to adequately deal with security threats. It is estimated [22], that in 2012, only 26% of companies with a security policy believed their staff understood how to use them.

It is necessary to recognise the magnitude of the threat environment. Attackers are constantly probing for weaknesses, which they will exploit without mercy. It is clear that the threat environment is developing just as quickly as the technological changes faced by industry [2] [25] [24]. We need to be aware of the threat this presents, be mindful of the fact that insider threats also pose a significant security risk, and try to minimise the possible impact. While we have absolutely no control over attackers, we can help reduce the impact by making life so difficult for them that they go away and attack an easier target instead. It is also necessary to understand that the threat environment is not restricted to outside actors. It is vital to understand that an equally dangerous threat may come from within the organisation. This can come in the form of employee laziness, incompetence, inexperience, lack of proper training, or worst of all, from malicious internal actors. This danger can be multiplied exponentially where they are acting in collusion with external malicious actors.

The above ten issues are of particular importance for management of a company, as they are the people responsible for determining the security position of the company, and enforcing the delivery of these goals. In the next sections, we consider a range of common mistakes made by management when adopting a cloud solution. Some of these mistakes are quite simple, some are more complex, but they all share a common thread, they all impact adversely on security.

III. Some Common Mistakes Companies Often Make When Transferring to Cloud

Companies should not believe the economic arguments of cloud service providers (CSPs) [56]. Instead, they should evaluate their needs properly for themselves, and where they are unsure, they should take neutral advice. It is necessary to prepare properly ahead of time, not to rush the decision to move to cloud, and to carry out their own due diligence on downtime history, data accessibility, pricing structure and CSP security and privacy record before signing any contract [57]. Companies should not assume it will be easy. Instead, they should think it through, understand the costs properly, and purchase the right service package rather than taking the first one that comes along [58].

Companies often wear cost blinkers when choosing cloud provisioning, but it is vital to factor in the risks and exposure too [59], not forgetting to just look at the short term, but to take the long view too. Before deciding, companies should check performance, making sure latency at end user nodes is acceptable. Remember, all clouds are not created equal. It is so important not to choose an inappropriate Cloud Service Provider (CSP).

Often, companies fail to prepare a proper disaster recovery plan [60]. Companies should always expect the unexpected, and plan for it. It is vital to be aware of what data must go to cloud, and who should be able to see it, and it is important not to forget access control. One key consideration is "location, location, location". Companies must understand where their data is stored [61], and how they can get their data back, if required. They need to understand who can gain access to their data. Cloud systems will not necessarily just be exposed to CSP personnel, but also other sub-contracted organisations [62], whose security and privacy approach may be nowhere near as good as that of the CSP. Companies often fail to account for data privacy risks. This presents a really good incentive for using encryption for their data.

When it comes to cloud security and privacy, there is no single solution [2]. In the first case, companies should not assume the CSP's security is good. CSPs have a heavy incentive not to release full details of previous security and privacy breaches so as not to adversely affect future sales. Companies should not use the wrong privacy approach, and should try to align security with its business goals [63]. Whatever approach is used, it must be cloud-friendly. For compliance, companies should always consider encryption [64], preferably with split encryption keys. Companies often sign up to cloud accepting the standard SLA. This can be a big mistake as many of these standard contracts are extremely vague about security and privacy, or do not even mention it. This lack of accountability on the part of the CSP will only help attackers breach company systems more easily.

When a company does switch to cloud, a common mistake is to try to do too much, too quickly. It is better to do small applications first, preferably those where failure will have minimal negative impact [65]. A company must not fail to understand the true threat against their employees, customers, suppliers and ultimately, their data. The company must have a cutting-edge comprehensive information security plan. The company needs to view security not just as an "IT problem", but rather as a "business problem" that also includes IT. Many who have implemented security as an IT problem have ended up with a strong IT implementation of data security controls but limited (if any) attention paid to the majority of available or required security controls such as physical security, security policies and procedures, training, and other administrative and environmental controls. People are generally the weakest link in the security chain, which is why special attention needs to be paid to their proper training in all security issues. This is also why security mirrors the business architecture of a company, people, process and technology [22], not technology alone.

It is also important for companies to "keep their eye on the ball", otherwise apathy soon follows, with consequent weakening of company security policies leading to disaster. Companies also need to keep up-to-date, by subscribing to threat intelligence feeds and collaborating with other leaders in the field [63]. New vulnerabilities and threats are discovered every day, and there is no room for complacency.

There have been a range of interesting approaches to try to alleviate some of the obvious issues in cloud security. One such area is the issue of how to ensure data integrity in the cloud. We see a number of interesting proposals, such as [66] [64] [67] [68] [69], which seek to provide assurance of data integrity to users through various forms of audit, which generally work quite well. There are those, such as [70] [71] [72] [73], who have suggested trust computing could be the way forward. Again, these can work well, but it is important to realise that despite establishing trust between providers and users, nevertheless, the fact remains that the work is being performed on someone else's systems, thus an element of risk will always remain. Others, such as [74] [75] [76] [77], believe provable data possession could help address this problem. Some believe that timeline entanglement, such as [78] [79] [80], is the way forward.

These systems, while generally proving capable of delivering what they promise, share a common flaw. They all provide an excellent means of achieving their objectives, but do not provide a means to deal with what happens after a serious security breach involving, usually brutal and indiscriminate, modification or deletion of multiple records. Where users do not understand the true purpose of an audit trail, it may be that they no longer have access to the necessary data with which to restore the modified or deleted data to its original state.

We can learn lessons from the accounting world, specifically in the area of the audit trail, as used with accounting systems for centuries. One of the key requirements in the accounting process is the separation of duties, and we discuss this more fully in the next section.

IV. The Importance of Separation of Duties

One of the core, long standing security concepts for internal business systems is that of "separation (or segregation) of duties." This concerns the advisability of separating and then parcelling out parts of a task to different people and places in order to reduce the opportunity for fraud or theft as multiple actors would need to take part. The fundamental nature of this concept is shown in the ground-breaking behavioural research of Ashton [81], who questioned auditors to seek an understanding of their consistency in applying judgement. He started with two questions in his questionnaire that embedded the concept of separation of duties

- Are the tasks of both timekeeping and payment of employees adequately separated from the task of payroll preparation?
- Are the tasks of both payroll preparation and payment of employees adequately separated from the task of payroll bank account?

The implications of judging that the answer to either of these two questions is "no" are obvious — an opportunity and a temptation arises for an individual to manipulate the payroll to their advantage. Clearly if it were possible to locate the payroll department away from the main work location and be confident that no one in payroll knew anyone in the rest of the company, then confidence would be increased yet further. Such separation not only makes fraud difficult, but also means unintentional errors are more likely to be spotted.

Gelinas et al. [82], pinpoint four basic transaction functions that should be separated: authorising transactions, executing transactions, recording transactions and safeguarding resources subsequent to the transactions being completed. Vaassen et al. [83], list five — "authorisation; custody; recording; checking and execution". Hall [84], takes the separation of duties logic and applies it specifically to computerised accounting, suggesting that the questions should now include "Is the logic of the computer program correct? Has anyone tampered with the application since it was last tested? Have changes been made to the programme that could have caused an undisclosed error?" (page 208). Whilst this may seem obvious and it might be assumed to be a problem that no longer causes grief, this is not the case. Ge and McVay [85], take advantage of the additional disclosures following the Sarbanes-Oxley Act [86], where executives were putting their lives on the line when signing off the integrity of their accounts, and examine companies that admit weaknesses. Looking at a two-year window (2002-2004) they find 261 firms with confessed internal control weaknesses and 45 of those admitted to a lack of segregation of duties. Computer firms were over-represented in the group of companies reporting problems.

The analogies to wider programming and software use are obvious and well known at least at a theoretical level. The more important question is whether the actual practice matches with the theory and then whether there is a record to demonstrate that such safety features were both in place and effective (i.e., the audit trail). As a real life example, one of the authors used to manage a large purchase ledger department and one of his staff got very confused with £2 million of invoices from a large supplier and had entered invoices, cancelled them, entered credit notes, cancelled them numerous times and had eventually come to him in tears. This was sorted, but the auditor some months later picked out these unusual transactions for investigation and an event log was able to show the mistakes, how they were rectified and who had performed each entry on the system.

We take a brief look at the current state of cloud security standards at the present time in order to demonstrate possible weaknesses in relying on compliance with these standards to provide cloud security assurance.

V. The Current State of Cloud Security Standards

There are a great many organisations who have worked on cloud security standards over the past decade. The following list, which is not exhaustive, gives a flavour of the variety of organisations working on the standards that are evolving today:

- AICPA [87];
  - AICPA Trust Service Criteria;
- ARTS [88];
- Basel 3 [89];
- BITS [90];
- CSA [32];
- CSCC [91];
- Control objectives for information and related technology (COBIT) [92];
- CSO [93];
- DPA [94];
- DMTF [95];
  - OVF;
  - OCSI;
  - CMWG;
  - CADFWG;
- ETSI [96];
  - TC Cloud;
  - CSC;
- FedRamp [97];
- Generally accepted privacy principles (GAPP) [98];
- GICTF [99];
- HIPAA [100];
- IATAC [101];
- ISACA [92];
  - COBIT;
- ISAE 3402 [102];
- ISO/IEC [103];
- Information technology infrastructure library (ITIL) [104];
- ITU [105];
- Jericho Forum [106];
- NIST [107];
- NERC [108];
  - CIP;
- OASIS [109];
  - OASIS Cloud-Specific or Extended TC;
    - OASIS CAMP TC;
    - OASIS ID Cloud TC;
    - OASIS SAF TC;
    - OASIS TOSCA TC;
    - OASIS CloudAuthZ TC;
    - OASIS PACR TC;
- OCC [110];
- OGF [111];
  - OCCI Working Group;
    - OCCI Core Specification;
    - OCCI Infrastructure Specification;
    - OCCI HTTP Rendering Specification;
    - Other OCCI-related Documents;
- OMG [112];
- PCIDSS [113];
- SNIA [114];
  - SNIA CDMI;
- The Open Group [115];
  - Cloud Work Group;
    - Cloud Computing Business Scenario;
    - Building Return on Investment from Cloud Computing;
- TM Forum [116];
  - Cloud Services Initiative;
    - TM Forum's Cloud Services Initiative Vision;
    - Barriers to Success;
    - ECLC Goals;
    - Future Collaborative Programs;
  - About the TM Forum;
    - TM Forum's Framework.

Most of these organisations have addressed specific cloud areas, particularly where they might relate to how their members might use cloud services with a better degree of safety. PCIDSS, for example, is specifically concerned with how cloud impacts on payment mechanisms. Larger organisations, such as CSA, ISACA, ISO/IEC, NIST tend to take a broader view to solving the problem. CSA and ISACA are cloud oriented organisations, while ISO/IEC and NIST have a much wider focus. Of the latter two, NIST were very quick to produce a cloud security standard, whereas the ISO/IEC standards approval process is very slow. On the plus side, once approved, an ISO/IEC standard will generally be adopted by large global corporates. To illustrate this process, NIST released their first cloud standard in 2009, followed in 2011 by a more comprehensive standard, which was well adopted by US corporates. Whereas, it took until 2014 before the ISO/IEC even mentioned cloud.

However, once they started moving, cloud standards started to flow, and ISO/IEC 27017:2015, which provides guidance for cloud specific security controls based on ISO/IEC 27002:2013, was finally approved in 2015. During the current decade, there has been a shift in the ISO 27000 series of standards from a compliance based approach to a risk based approach, and this is to be welcomed. ISO/IEC 27018:2014 was published in 2014, and covers use of personally identifiable information (PII) in public clouds. ISO/IEC 270364:2016 provides guidance on the security of cloud services. This standard does not address business continuity management or resiliency issues for cloud services. These are addressed in ISO/IEC 27031:2011, although this has been improved on in ISO 22301:2012.

There are three security studies currently being conducted by the ISO/IEC on: cloud security assessment and audit; cloud-adapted risk management framework; and cloud security components. Beyond that, the following four areas have been proposed: guidelines for cloud service customer data security; the architecture of trusted connection to cloud services; the architecture for virtual root of trust on cloud platforms; and emerging virtualization security.

Thus we will next take a brief look at cloud audit literature to see what lessons we can learn from this area.

VI. Cloud Audit Literature

Vouk [117], in an early description of the issues surrounding cloud computing, suggests there must be an ability to audit processes, data and processing results. By 2009, we see a little more concern being expressed in the area of cloud audit. Wang et al. [118] 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), on behalf of the cloud client, to verify the integrity of the dynamic data stored in the cloud. The authors identify the difficulties and potential security problems and show how to construct an elegant verification scheme for seamless integration of these features into protocol design.

Leavitt [119] 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, a a line of enquiry they generally discourage. Some CSPs are addressing this by appointing TPAs to audit their systems in advance and by documenting procedures designed to address customers data security needs. Where the TPA is not an accounting firm, there may be some question as to auditor impartiality. Bernstein et al. [120] 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, and suggests some kind of audit-ability would be needed. The authors stress the need for cloud systems to provide strong and secure audit trails.

Pearson and Benameur [121] recognise that achieving proper audit trails in the cloud is an unresolved issue. Wang et al. [122] address privacy preserving public auditing for data storage security in cloud, and are keen to prevent TPA introduced weaknesses to the system. The authors present a mechanism to enable a more secure approach to public audit by TPAs. Zhou et al. [123] carry out a survey on security and privacy in cloud computing, and investigate several CSPs about their concerns on security and privacy issues, finding 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. Chen and Yoon [60] 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.

Armbrust et al. [124] present a detailed description of what cloud computing is, and note that the possible lack of auditability presents the number three barrier to implementation. Ramgovind et al. [125] 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 take up. Grobauer et al. [126] 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 good cloud audit practice can be provided to ensure proper security is achieved.

Doelitzscher et al. [127] present a prototype demonstration of Security Audit as a Service (SAaaS) architecture, a cloud audit system that 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 [128] 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.

Pappas et al. [129] 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. Xie and Gamble [30] outline a tiered approach to auditing information in the cloud. The approach provides perspectives on audit-able events that may include compositions of independently formed audit trails. Zhu et al. [77] 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.

Ruebsamen and Reich [130] 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. Doelitzscher et al. [131] propose the use of neural networks to analyse and learn the normal usage behaviour of cloud customers, so that anomalies originating 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. [132] 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. [133] 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. Wang et al. [134] 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.

Lopez et al. [135] 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. Shameli-Sendi and Cheriet [136] propose a framework for assessing the security risks associated with cloud computing platforms. Xiong and Chen [137] consider how to allocate sufficient computing resources but not to over-provision these resources 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.

Now that we have looked at the cloud audit literature, will take a look at the audit trail in a bit more depth, to gain a better understanding of the detail we need to get to grips with to help us gain some benefit from it.

VII. 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 and a number of problems are yet to be resolved. Duncan and Whittington [2] 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 an alternate 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 professional mind-sets 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) [138] 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 that 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". As we can see, there is not a complete common understanding between the two disciplines of what an audit trail should be able to achieve.

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 is subjected to. Some 20 years ago, the National Institute of Standards and Technology (NIST) [139] 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. However, 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 [120] suggests the audit trail comprises: events, logs, and analysis thereof, Chaula [140] suggests: raw data, analysis notes, preliminary development and analysis information, processes notes, etc.

Pearson et al. [121] recognise that achieving proper audit trails in the cloud is an unresolved issue. Ko et al. [141] explicitly note that steps need to be taken to prevent audit trails disappearing after a cloud instance is shut down. Ko [142] 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 [143] raises several cloud-specific security risks, such as loss of governance, insecure or incomplete data deletion, insufficient audit trails or isolation failures, which are not sufficiently addressed by the 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 IT people, as an unnecessary duplication, will prove invaluable in the event of compromise. One of the authors has spoken to countless IT people who have claimed they already have multiple backups of all their data, so do not see the need for a proper audit trail. This completely misses the point that after a breach occurs, the corrupted data will be duplicated over time into all the carefully maintained backup copies, resulting in multiple sets of corrupted data. This is particularly problematic where there is a considerable time between breach and discovery. Whereas, a simple, carefully protected audit trail would allow the corrupted system to be fully reconstructed.

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 [141], unless steps are taken to prevent their loss. In real world conditions, most database software ships with inadequate audit trail provision in the default settings. Anderson [144] states that the audit trail should only be capable of being read by users rather than being edited. 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 elses hardware — the CSPs. These CSPs also employ system administrators. CSPs also employ temporary staff from time to time, some of whom are also system administrators. While the CSP may vet their own staff to a high level, this may not the case with temporary employees [146]. Network connections too are often virtualized, 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 elses hardware, and often software too — the CSPs. The cloud relationship needs to include the CSP as a key partner in the pursuit of achieving security [6]. Unless and until CSPs are willing to share this goal, technical solutions will be doomed to failure.

Thus in the next section, we will take a look at some of the practical approaches we can take to help us achieve the goal of a better level of security. Most of these recommendations will not be technically challenging, yet many companies fail to act on these simple actions, which could significantly improve security for their company.

VIII. How can we improve the audit trail?

There are three fundamental weaknesses here, which need to be addressed. 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.

To illustrate the first point, we discuss one of the most popular open source database programmes in general use today — MySQL. The vast majority of implementations will use either standard default settings on installation, or install the programme as part of a standard Linux, Apache, MySQL and PHP (LAMP) server. In the case of 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 whole purpose of a LAMP server. Unfortunately this does not adequately address security in each of the four elements of the LAMP server.

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:

- 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.

Turning to the second point, as Anderson [144] 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 has been subject to lesser scrutiny.

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 that relate to their intrusion of the system, or to simply delete the entire audit trail files. And, when the instance is shut down, all the data disappears anyway.

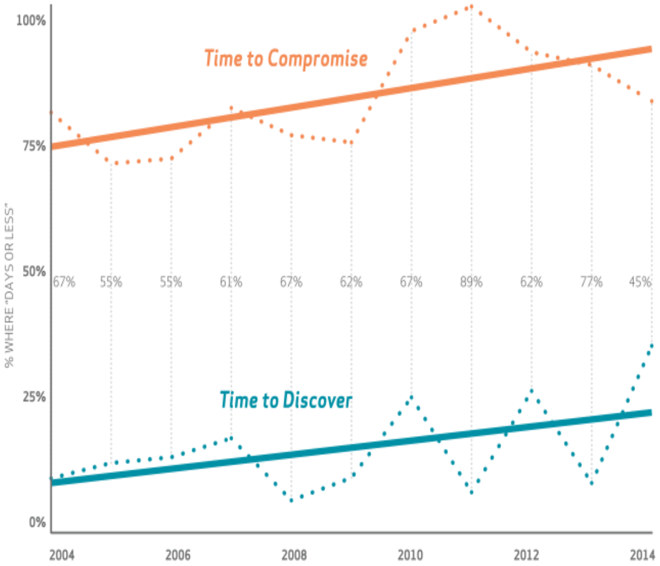
These three points are generally not much thought about, yet they present a serious weakness to the success of maintaining the audit trail. Equally, these are relatively trivial to address. Often management and IT staff will take the view "so what?".

Simply turn on data logging and send 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 again, this should be run on an independent secure server under the control of the cloud user. The use of an audit plug-in in addition to all the basic logging capabilities, is also a useful thing to do. While there will be an element of double processing involved, it is better to have more data than none at all.

Where the MySQL instance forms part of a LAMP server, then it would also 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 as far back as 2012, Trustwave [145], report an average of 6 months between breach and discovery. It is also rather worrying to see that three years later [147], see Fig. 1, that 75% of breaches happen within days, yet only 25% of discoveries are actually made within the same time-frame. This still leaves a large gap where compromised systems may still be under the control of malicious users.

Fig. 1. The Lag Between Breach and Discovery © 2015 Verizon



This presents a clear indication that very few firms are actually scrutinising their server logs. Back in 2012, Verizon [53] highlighted the fact that discovery of security breaches often took weeks, months or even years before discovery, with most discovery being advised by external bodies, such as customers, financial institutions or fraud agencies.

The Open Web Application Security Project (OWASP) carry out a survey every 3 years in which they collate the number of vulnerabilities with the greatest impact on companies. In TABLE I we can see the top ten list from 2013, 2010 and 2007:

TABLE I. OWASP Top Ten Web Vulnerabilities — 2013 [148]

2013	2010	2007	Threat
1	1	2	Injection Attacks
2	3	7	Broken Authentication and Session Management
3	2	1	Cross Site Scripting (XSS)
4	4	4	Insecure Direct Object References
5	6	-	Security Misconfiguration
6	-	-	Sensitive Data Exposure
7	-	-	Missing Function Level Access Control
8	5	5	Cross Site Request Forgery (CSRF)
9	-	-	Using Components with Known Vulnerabilities
10	-	-	Unvalidated Redirects and Forwards

Sitting at the top of the table for 2013, again for 2010, and in second place in 2007, we have injection attacks. It is very clear that companies are consistently failing to configure their database systems properly. Injection attacks rely on misconfigured databases used in dynamic web service applications, which allow SQL, OS, or LDAP injection to occur when untrusted data is sent to an interpreter as part of a command or query. The attackers hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization. This can lead to compromise, or deletion of data held in company databases.

SQL injection attacks are relatively straightforward to defend against. OWASP provide an SQL injection prevention cheat sheet [149], in which they suggest a number of defences:

- Use of Prepared Statements (Parameterized Queries);
- Use of Stored Procedures;
- Escaping all User Supplied Input;

They also suggest that companies should enforce least privilege and perform white list input validation as useful additional precautions to take.

For operating system injection flaws, they also have a cheat sheet [150], which suggests that LDAP injection attacks are common due to two factors, namely the lack of safer, parameterized LDAP query interfaces, and the widespread use of LDAP to authenticate users to systems. Their recommendations for suitable defences are:

- Rule 1 Perform proper input validation;
- Rule 2 Use a safe API;
- Rule 3 Contextually escape user data.

And for LDAP system injection flaws, their cheat sheet [151], recommends the following injection prevention rules:

- Defence Option 1: Escape all variables using the right LDAP encoding function;
- Defence Option 2: Use Frameworks that Automatically Protect from LDAP Injection.

None of these preventative measures suggested by OWASP are particularly difficult to implement, yet judging by the recurring success of these simple attacks, companies are clearly failing to take even simple actions to protect against them.

When considering secure audit trail and system logging for a database, there are a number of simple configuration options open to the user. First, applying the above OWASP recommendations would considerably limit exposure. Looking at the database itself, the user access for posting records to the logging database can have the option to modify or delete records disabled. On the plus side, full database capabilities are retained. On the negative side, should an attacker be able to gain access to the database, and subsequently be able to escalate privileges, then these restrictions could be reversed, thus exposing the database.

Another simpler approach would be to configure the database as an archive database. This allows new records to be added, prevents modification of records in the database, and also prevents deletion of records. On the plus side, the attacker cannot change the database type, but on the negative side, the database cannot be indexed, thus making searching more difficult (time consuming).

Yet another possibility would be to configure the database such that full facilities are retained, but with the modify and delete commands completely removed. This would meet the goals for a proper audit trail, and would provide the ability to retain full search capabilities for rapid analysis and searching of the audit trail.

Thus, in addition to making the simple suggestions we propose above, cloud users should also make sure they actually review these audit trail logs. It is vital to be able to understand when a security breach has occurred, and exactly which records have been accessed, compromised or stolen. While recognising that this is not a foolproof method of achieving cloud security, it is likely to present a far higher level of affordable, achievable security than many companies currently achieve.

However, we must warn that even if a company implements these simple suggestions, that still will not guarantee security. While it will annoy the majority of attackers to such an extent that they will move on to easier pickings, it may well be that new vulnerabilities will arise. Therefore the company must remain vigilant at all times. It would be prudent to subscribe to security feeds, and follow leaders in the field to ensure they remain aware of all the latest security vulnerabilities and exploits. Of course, companies must also realise that the threat environment is not restricted to outside parties alone. Perhaps of greater concern is the threat posed by malicious internal actors, which can be even more serious where they act in concert with outside parties. This presents one of the most serious weaknesses to the security of a company. Equally, laziness on the part of staff or lack of knowledge, particularly where they have not been regularly trained to provide them with full awareness of all the latest threats, including social engineering attacks, and the consequence of falling victim to them, can also pose an extremely serious risk to company security.

In the event of a security breach, not if, but rather when it happens, it may be necessary to conduct a forensic examination to establish how the company defences were breached. With traditional distributed systems, there is usually something for the forensic computer scientists to find, somewhere in the system. They are completely accustomed to dealing with being able to find only partial traces of events, from which they can build a forensic picture of the breach. This becomes more problematic the longer the time between breach and discovery.

However, once a company adopts cloud use, this becomes far more problematic. While forensic computer scientists can work wonders with a range of partial discoveries, deleted or otherwise, once a cloud instance is shut down, there is virtually zero chance of regaining access to the shut down system. The disk space used by that system could be re-used, literally within seconds, and where the time interval between breach and discovery is considerably longer, as is generally the norm, then this opportunity becomes a physical impossibility. Thus, for forensic purposes, companies need to pay far more attention to what is actually going on in the cloud.

In the next Section, we provide a number of tables as a reminder of the issues we have discussed in this article and how to attempt to mitigate these issues.

IX. A Reminder on Who is Responsible to Mitigate the Problem Areas

In this Section, we provide some tables as a handy reminder of who is responsible for ensuring the mitigation of problem areas. We start, in TABLE II, by taking a look at the 10 key management risk areas we discussed in Section II.

TABLE II. 10 Key Management Risk Areas Weaknesses and Mitigating Responsibilities ©2016 Duncan and Whittington

Item	Weakness	Responsibility for Mitigation
1	Definition of Security Goals	Management
2	Standards Compliance	Management
3	Audit Issues	Management and Internal Audit
4	Management Approach	Management
5	Technical Complexity	Management and IT
6	Lack of Responsibility	Management
7	Measurement and Monitoring	Management and IT
8	Management Attitude to Security	Management
9	Security Culture	Management and All Employees
10	Threat Environment	Extreme Vigilance by Management and IT

Clearly, since these are key management risk areas, management must necessarily take a heavy responsibility for ensuring these areas are properly dealt with. First, the definition of clear security goals provides the fundamental basis for ensuring a good security posture can be achieved by the company. Note, there should be no delegation of this vital task to IT. Management must take full ownership of this task. On the matter of standards compliance, management must understand that since cloud security standards are not yet complete, they must recognise the risks involved in attempting to rely on this compliance for security. Management must also recognise the shortcomings pertaining to audit methodology, and should do so in conjunction with internal audit, and, if necessary, in consultation with the external auditors.

Management need to recognise the impact of the management approaches adopted by all cloud actors, and recognise how these differing approaches and risk appetites can increase risk to the company. Management, in conjunction with their IT department, must explicitly understand the potential impact due to the added complexity of cloud ecosystems, in order to ensure proper mitigation is achieved. Management must also recognise the potential impact brought about through a lack of responsibility and accountability from all the actors in the cloud ecosystem chain, including their own staff.

Management must recognise fully the need for establishing proper metrics in order to ensure proper measurement and monitoring can take place. In this way, there will at least be a recognition of when an attack has occurred, thus providing an opportunity to ensure mitigating steps are immediately taken. Management need to ensure they take a serious attitude towards security, preferably with a board member being appointed as the responsible security board member of the company. This will help to ensure a proper security culture can be developed, and maintained within the company.

Finally, there is a pressing need for management to take very seriously the potential danger posed by the threat environment. By ensuring that currently known vulnerabilities are quickly identified and mitigating action is taken promptly, this will help reduce the impact posed by the threat environment. Obviously, new vulnerabilities will become exposed all the time, and with the previous steps taken, and in particular extreme levels of vigilance, this should help to mitigate the overall danger posed.

In TABLE III, we consider the common mistakes companies often make when adopting cloud computing within their organisation, as we discussed in Section III.

TABLE III. COMMON MISTAKES
WEAKNESSES AND MITIGATING STRATEGIES ©2016 DUNCAN AND WHITTINGTON

Item	Weakness	Action Required
1	CSP Sales Talk	Do not believe the hype. Do your own due diligence
2	Business Continuity	Prepare a proper disaster recovery plan
3	Cloud Security	Remember, there is no single solution
4	Rapid Deployment	Don't try to do it all at once
5	Ongoing Ennui	Do not relax. Be vigilant at all times
6	Other Approaches	Look out for the loopholes
7	After a Breach	Have a plan for what to do after a breach

Remember, the primary goal of the CSP is get your signature on the contract. Take nothing at face value, and scrutinise the small print very carefully. What will you do in the event of a security breach? You must have a proper and comprehensive disaster recovery plan in place before you start using cloud. Later will be too late. Do not forget that there is no single solution to cloud security. Identify the risks, take mitigating steps and above all remain vigilant at all times.

Do not try to implement your cloud installation too quickly. You need to thoroughly carry out security testing to ensure you eliminate as many issues as possible before you commit fully to the system. Once it is up and running, do not assume all will be well for evermore.

Do not assume new approaches will be a perfect solution to the problem. There will likely be one or more loopholes involved. Make sure that you are the one to find them. Above all else, have a plan in place for what to do the moment you have a breach. With cloud systems, you cannot afford to wait while you develop a plan. You have to take action right away, otherwise there might be very little for you to investigate where cloud systems are in use.

With regard to separation of duties, as discussed in Section IV, it is worth remembering that this advice can and should be applied to people, processes and technology. This will ensure proper internal control can be organised across the whole of the business architecture of the company.

When it comes to cloud security standards, as covered in Section V, remember there is no complete cloud security standard yet in existence, and often, the compliance mechanisms can be flawed, leading to a false sense of security evolving. Guard against this arising at all costs.

Finally, do not forget the benefits to be obtained from implementing a proper audit trail. In TABLE IV, we reiterate the main points addressed in Section VIII.

TABLE IV. POSSIBLE IMPROVEMENTS TO ENSURE
A COMPLETE AUDIT TRAIL ©2016 DUNCAN AND WHITTINGTON

Item	Weakness	Action Required
1	Inadequate Default Logging	Make sure adequate logging is turned on
2	Insecure Audit Trail Data	Protect access to this data properly
3	Incomplete Audit Trail Data	Ensure full data collection
4	Secure Audit Trail	Use a separate secure server for this
5	Secure Server Setup	Setup a hardened server
6	Securing the Audit Trail Server	Add an Intrusion Detection system
7	Ensuring Security	Setup a live monitoring system
8	Ensuring Security	Update all security patches regularly
9	Ensuring Security	Setup immutable databases for the audit trail
10	Ensuring Security	Collect data from all running cloud instances

There is a great deal of work that can be carried out with databases to ensure a more robust environment is used to limit the damage from any security breach that might occur. It is vital to ensure that taking the easy option of using default settings is never to be allowed to happen. Default settings, while very easy to implement, are a vital security weakness which can be a great enabler for the attacker. A company should always take the trouble to take this treat away from potential attackers.

In the next section, we shall review our findings and discuss our conclusions.

X. 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 issues with cloud security standards, and how that might impact on cloud security. We have considered how the lack of accountability can impact on security. We have discussed how a number of the above issues must additionally be addressed. It is clear that companies who use cloud need to understand the impact that the complexities of using cloud will have on their security will have to be very carefully considered in order to ensure they do not fall foul of the many opportunities that exist for security controls to "fall down the gaps" and thus become lost forever.

The practice of using default settings when installing software in a cloud environment is clearly asking for trouble. These simple steps we propose 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 will certainly prove beneficial. Examination of the logs need not be challenging or costly — there are many software solutions available to address this task using programmatic means. 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 than can really help improve security are ignored.

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. 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, “Enhancing Cloud Security and Privacy: The Power and the Weakness of the Audit Trail,” in *Cloud Comput. 2016 Seventh Int. Conf. Cloud Comput. GRIDs, Virtualization*. Rome: IEEE, 2016, pp. 125–130.

[2] 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.

[3] B. Duncan, D. J. Pym, and M. Whittington, “Developing a Conceptual Framework for Cloud Security Assurance,” in *Cloud Comput. Technol. Sci. (CloudCom), 2013 IEEE 5th Int. Conf. (Volume 2)*. Bristol: IEEE, 2013, pp. 120–125.

[4] N. Papanikolaou, S. Pearson, M. C. Mont, and R. K. L. Ko, “Towards Greater Accountability in Cloud Computing through Natural-Language Analysis and Automated Policy Enforcement,” *Engineering*, pp. 1–4, 2011.

[5] A. Baldwin, D. Pym, and S. Shiu, “Enterprise Information Risk Management: Dealing with Cloud Computing,” *Abdn.Ac.Uk*, pp. 257—-291, 2013.

[6] B. Duncan and M. Whittington, “Enhancing Cloud Security and Privacy: Broadening the Service Level Agreement,” in *14th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. (IEEE Trust.*, Helsinki, Finland, 2015, pp. 1088–1093.

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

[8] A. Gill, “Corporate Governance as Social Responsibility: A Research Agenda,” *Berkeley J. Int’l L.*, vol. 26, no. 2, pp. 452–478, 2008.

[9] 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.

[10] A. Kolk, “Sustainability, accountability and corporate governance: Exploring multinationals’ reporting practices.” *Bus. Strateg. Environ.*, vol. 17, no. 1, pp. 1–15, 2008.

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

[12] S. Arjoon, “Corporate Governance: An Ethical Perspective,” *J. Bus. Ethics*, vol. 61, no. 4, pp. 343–352, nov 2012.

[13] B. Duncan and M. Whittington, “Reflecting on whether checklists can tick the box for cloud security,” in *Proc. Int. Conf. Cloud Comput. Technol. Sci. CloudCom*, vol. 2015-Febru, no. February. Singapore: IEEE, 2015, pp. 805–810.

[14] B. Duncan and M. Whittington, “The Importance of Proper Measurement for a Cloud Security Assurance Model,” in *2015 IEEE 7th Int. Conf. Cloud Comput. Technol. Sci.*, Vancouver, 2015, pp. 1–6.

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

[16] E. Humphreys, “Information security management standards: Compliance, governance and risk management,” *Inf. Secur. Tech. Rep.*, vol. 13, no. 4, pp. 247–255, Nov 2008.

[17] F. Albersmeier, H. Schulze, G. Jahn, and A. Spiller, “The reliability of third-party certification in the food chain: From checklists to risk-oriented auditing,” *Food Control*, vol. 20, no. 10, pp. 927–935, 2009.

[18] K. Prislan and I. Bernik, “Risk Management with ISO 27000 standards in Information Security,” *Inf. Secur.*, pp. 58–63, 2010.

[19] IsecT, “Information Security Frameworks from ”Audit” to ”Zachman”,” Tech. Rep. March, 2011.

[20] Order, “Executive Order 13636: Improving Critical Infrastructure Cybersecurity,” pp. 1–8, 2013.

[21] B. Duncan and M. Whittington, “Enhancing Cloud Security and Privacy: The Cloud Audit Problem,” in *Cloud Comput. 2016 Seventh Int. Conf. Cloud Comput. GRIDs, Virtualization*. Rome: IEEE, 2016, pp. 119–124.

[22] PWC, “UK Information Security Breaches Survey - Technical Report 2012,” London, Tech. Rep. April, 2012. [Online]. Available: www.pwc.comwww.bis.gov.uk [Last Accessed: 30 Nov 2016]

[23] T. Sang, “A Log-based Approach to Make Digital Forensics Easier on Cloud Computing,” *Proc. 2013 3rd Int. Conf. Intell. Syst. Des. Eng. Appl. ISDEA 2013*, pp. 91–94, 2013.

[24] B. Duncan and M. Whittington, “Information Security in the Cloud: Should We be Using a Different Approach?” in *2015 IEEE 7th Int. Conf. Cloud Comput. Technol. Sci.*, Vancouver, 2015, pp. 1–6.

[25] 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. 154–159.

[26] E. Zio, “Reliability engineering: Old problems and new challenges,” *Reliab. Eng. Syst. Saf.*, vol. 94, no. 2, pp. 125–141, Feb 2009.

[27] 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 [Last Accessed: 30 Nov 2016]

[28] M. Theoharidou, N. Papanikolaou, S. Pearson, and D. Gritzalis, “Privacy Risk , Security , Accountability in the Cloud,” in *IEEE Int. Conf. Cloud Comput. Technol. Sci. Priv.*, 2013, pp. 177–184.

[29] C. Millard, I. Walden, and W. K. Hon, “Who is Responsible for ’Personal Data’ in Cloud Computing? The Cloud of Unknowing, Part 2,” *Leg. Stud.*, vol. 27, no. 77, pp. 1–31, 2012.

[30] S. Pearson, “Taking account of privacy when designing cloud computing services,” *Proc. 2009 ICSE Work. Softw. Eng. Challenges Cloud Comput. CLOUD 2009*, pp. 44–52, 2009.

[31] S. Pearson and A. Charlesworth, “Accountability as a way forward for privacy protection in the cloud,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 5931 LNCS, no. December, pp. 131–144, 2009.

[32] C. C. V, “Security research alliance to promote network security,” Cloud Security Alliance, Tech. Rep. 2, 1999. [Online]. Available: http://scholar.google.com/scholar?hl=en{\&}btnG=Search{\&}q=intitle:Security+Guidance+Critical+Areas+of+Focus+for{\#}0 [Last Accessed: 30 Nov 2016]

[33] T. Hahn, F. Figge, J. Pinkse, and L. Preuss, “Editorial Trade-Offs in Corporate Sustainability: You Can’t Have Your Cake and Eat It,” *Bus. Strateg. Environ.*, vol. 19, no. 4, pp. 217–229, 2010.

[34] A. Lindgreen and V. Swaen, “Corporate Social Responsibility,” *Int. J. Manag. Rev.*, vol. 12, no. 1, pp. 1–7, 2010.

[35] D. J. Wood, “Measuring Corporate Social Performance: A Review,” *Int. J. Manag. Rev.*, vol. 12, no. 1, pp. 50–84, 2010.

[36] T. Green and J. Peloza, “How does corporate social responsibility create value for consumers?” *J. Consum. Mark.*, vol. 28, no. 1, pp. 48–56, 2011.

[37] A. Christofi, P. Christofi, and S. Sisaye, “Corporate sustainability: historical development and reporting practices,” *Manag. Res. Rev.*, vol. 35, no. 2, pp. 157–172, 2012.

[38] N. Rahman and C. Post, “Measurement Issues in Environmental Corporate Social Responsibility (ECSR): Toward a Transparent, Reliable, and Construct Valid Instrument,” *J. Bus. Ethics*, vol. 105, no. 3, pp. 307–319, 2012.

[39] M. A. Delmas, D. Etzion, and N. Nairn-Birch, “Triangulating Environmental Performance: What Do Corporate Social Responsibility Ratings Really Capture?” *Acad. Manag. Perspect.*, vol. 27, no. 3, pp. 255–267, 2013.

[40] I. Montiel and J. Delgado-Ceballos, “Defining and Measuring Corporate Sustainability: Are We There Yet?” *Organ. Environ.*, vol. Advance on, pp. 1–27, 2014.

[41] D. Bodeau, R. Graubart, L. LaPadula, P. Kertzner, A. Rosenthal, and J. Brennan, “Cyber Resiliency Metrics ,,” *MITRE Rep. MP 120053 Rev 1.*, no. April, pp. 1–40, 2012.

[42] H. Carvalho, S. G. Azevedo, and V. Cruz-Machado, “Agile and resilient approaches to supply chain management: influence on performance and competitiveness,” *Logist. Res.*, vol. 4, no. 1-2, pp. 49–62, 2012.

[43] M. Vieira, H. Madeira, K. Sachs, and S. Kounev, “Resilience Benchmarking,” *Resil. Assess. Eval. Comput. Syst.*, pp. 283–301, 2012.

[44] A. V. Lee, J. Vargo, and E. Seville, “Developing a Tool to Measure and Compare Organizations’ Resilience,” *Nat. Hazards Rev.*, no. February, pp. 29–41, 2013.

[45] I. Linkov, D. A. Eisenberg, M. E. Bates, D. Chang, M. Convertino, J. H. Allen, S. E. Flynn, and T. P. Seager, “Measurable Resilience for Action-

able Policy," *Environ. Sci. Technol.*, vol. 47, no. ii, p. 130903081548008, 2013.

[46] I. Linkov, D. A. Eisenberg, K. Plourde, T. P. Seager, J. Allen, and A. Kott, "Resilience metrics for cyber systems," *Environ. Syst. Decis.*, vol. 33, no. 4, pp. 471–476, 2013.

[47] T. Prior and J. Hagmann, "Measuring resilience: methodological and political challenges of a trend security concept," *J. Risk Res.*, vol. 17, no. 3, pp. 281–298, 2014.

[48] C. Ioannidis, D. Pym, J. Williams, and I. Gheyas, "Resilience in Information Stewardship," in *Weis 2014*, vol. 2014, no. June, 2014, pp. 1–33.

[49] K. Gilman and J. Schulschenk, "Sustainability Accounting Standards Board," pp. 14–17, 2012. [Online]. Available: www.sasb.org [Last Accessed: 30 Nov 2016]

[50] R. Eccles, K. Perkins, and G. Serafeim, "How to Become a Sustainable Company," *MIT Sloan Manag. Rev.*, vol. 53, no. 4, pp. 43–50, 2012.

[51] R. G. Eccles, I. Ioannou, and G. Serafeim, "The Impact of Corporate Sustainability on Organizational Processes and Performance," *Manage. Sci.*, vol. 60, no. 11, pp. 2835–2857, 2014.

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

[53] Verizon, N. High, T. Crime, I. Reporting, and I. S. Service, "2012 Data Breach Investigations Report," Verizon, Tech. Rep., 2012.

[54] ISACA, "An Introduction to the Business Model for Information Security," Tech. Rep., 2009.

[55] PWC, "Information Security Breaches Survey 2010 Technical Report," pp. 1–22, 2010.

[56] M. Armbrust, I. Stoica, M. Zaharia, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, and A. Rabkin, "A View of Cloud Computing: Clearing the clouds away from the true potential and obstacles posed by this computing capability." *Commun. ACM*, vol. 53, no. 4, pp. 50–58, 2010.

[57] J. Opara-Martins, R. Sahandi, and F. Tian, "Critical review of vendor lock-in and its impact on adoption of cloud computing," *Int. Conf. Inf. Soc. i-Society 2014*, pp. 92–97, 2015.

[58] Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: State-of-the-art and research challenges," *J. Internet Serv. Appl.*, vol. 1, no. 1, pp. 7–18, 2010.

[59] K. Dahbur, B. Mohammad, and A. B. Tarakji, "A Survey of Risks, Threats and Vulnerabilities in Cloud Computing," *Computing*, pp. 1–6, 2011.

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

[61] D. J. Abadi, "Data management in the cloud: limitations and opportunities," *IEEE Data Eng. Bull.*, vol. 32, no. 1, pp. 3–12, 2009.

[62] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, and J. Molina, "Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control," in *Proc. 2009 ACM Work. Cloud Comput. Secur.*, 2009, pp. 85–90.

[63] K. Popovic and Z. Hocenski, "Cloud computing security issues and challenges," *MIPRO, 2010 Proc. 33rd Int. Conv.*, pp. 344–349, 2010.

[64] S. Subashini and V. Kavitha, "A Survey on Security Issues in Service Delivery Models of Cloud Computing," *J. Netw. Comput. Appl.*, vol. 34, no. 1, pp. 1–11, 2011.

[65] C. Low, Y. Chen, and M. Wu, "Understanding the determinants of cloud computing adoption," *Ind. Manag. Data Syst.*, vol. 111, no. 7, pp. 1006–1023, 2011.

[66] Z. Hao, S. Zhong, and N. Yu, "A Privacy-Preserving Remote Data Integrity Checking Protocol with Data Dynamics and Public Verifiability," *IEEE Trans. Knowl. Data Eng.*, vol. 23, no. 9, pp. 1432–1437, 2011.

[67] D. Chen and H. Zhao, "Data Security and Privacy Protection Issues in Cloud Computing," *2012 Int. Conf. Comput. Sci. Electron. Eng.*, vol. 1, no. 973, pp. 647–651, 2012.

[68] K. Yang and X. Jia, "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing," *IEEE Trans. Parallel Distrib. Syst.*, vol. I, no. 9, pp. 2–5, 2014.

[69] L. Wei, H. Zhu, Z. Cao, X. Dong, W. Jia, Y. Chen, and A. V. Vasilakos, "Security and privacy for storage and computation in cloud computing," *Inf. Sci. (Ny).*, vol. 258, pp. 371–386, 2014.

[70] N. Santos, K. P. Gummadi, and R. Rodrigues, "Towards Trusted Cloud Computing," *Inf. Secur. Tech. Rep.*, vol. 10, no. 2, p. 5, 2005.

[71] Z. Shen, L. Li, F. Yan, and X. Wu, "Cloud Computing System Based on Trusted Computing Platform," *2010 Int. Conf. Intell. Comput. Technol. Autom.*, pp. 942–945, 2010.

[72] S. Sengupta, V. Kaulgud, and V. S. Sharma, "Cloud Computing Security - Trends and Research Directions," *2011 IEEE World Congr. Serv.*, no. October, pp. 524–531, 2011.

[73] Z. Xiao and Y. Xiao, "Security and Privacy in Cloud Computing," *Commun. Surv. Tutorials, IEEE*, vol. 15, no. 2, pp. 843–859, 2013.

[74] Y. Zhu, H. Wang, Z. Hu, G.-j. Ahn, H. Hu, S. S. Yau, H. I. Storage, and R. Information, "Efficient Provable Data Possession for Hybrid Clouds," in *Proc. 17th ACM Conf. Comput. Commun. Secur.*, 2010, pp. 756–758.

[75] G. Ateniese, R. Burns, R. Curtmola, J. Herring, O. Khan, L. Kissner, Z. Peterson, and D. Song, "Remote data checking using provable data possession," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, pp. 1–34, 2011.

[76] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing," in *IEEE Trans. Parallel Distrib. Syst.*, vol. 22, no. 5, 2011, pp. 847–859.

[77] Y. Zhu, H. Hu, G. J. Ahn, and M. Yu, "Cooperative provable data possession for integrity verification in multicloud storage," in *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 12, 2012, pp. 2231–2244.

[78] H. T. T. Truong, C.-L. Ignat, and P. Molli, "Authenticating Operation-based History in Collaborative Systems," *Proc. 17Th Acm Int. Conf. Support. Gr. Work*, pp. 131–140, 2012.

[79] M. Mizan, M. L. Rahman, R. Khan, M. Haque, and R. Hasan, "Accountable proof of ownership for data using timing element in cloud services," *Proc. 2013 Int. Conf. High Perform. Comput. Simulation, HPCS 2013*, pp. 57–64, 2013.

[80] S. L. Reed, "Bitcoin Cooperative Proof of Stake," pp. 1–16, 2014.

[81] R. H. Ashton, "An experimental study of internal control judgements," *J. Account. Res.*, pp. 143–157, 1974.

[82] S. S. G. Gelinas U.J. and A. E. Oram, *Accounting Information Systems (4th edition)*. South-Western College Publishing, Cincinnati, Ohio, US., 1999.

[83] E. Vaassen, R. Meuwissen, and C. Schelleman, *Accounting information systems and internal control*. Wiley Publishing, 2009.

[84] J. A. Hall, *Accounting Information Systems (3rd edition)*. South-Western College Publishing, Cincinnati, Ohio, US., 2001.

[85] W. Ge and S. McVay, "The disclosure of material weaknesses in internal control after the Sarbanes-Oxley Act," *Account. Horizons*, vol. 19, no. 3, pp. 137–158, 2005.

[86] Sox, "Sarbanes-Oxley Act of 2002," p. 66, 2002.

[87] AICPA, "AICPA SOC2 Standard," 2014. [Online]. Available: https://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/AICPASOC2Report.aspx [Last Accessed: 30 Nov 2016]

[88] ARTS, "Association for Retail Technology Standards," 2014. [Online]. Available: https://nrf.com/resources/retail-technology-standards-0 [Last Accessed: 30 Nov 2016]

[89] Basel3, "Basel 3 Impact," Basel, Tech. Rep. December 2010, 2011. [Online]. Available: http://www.bis.org/bcbs/basel3.htm?m=3\%257C14\%257C572 [Last Accessed: 30 Nov 2016]

[90] BITS, "Financial Services Roundtable Standards," Tech. Rep. [Online]. Available: http://www.bits.org/ [Last Accessed: 30 Nov 2016]

[91] CSCC, "Cloud Standards Customer Council," 2015. [Online]. Available: http://http://www.cloud-council.org/ [Last Accessed: 30 Nov 2016]

[92] ISACA, "Planning for and Implementing ISO 27001," *ISACA J.*, vol. 4, 2011. [Online]. Available: http://www.isaca.org/Journal/Past-Issues/2011/Volume-4/Documents/jpdf11v4-Planning-for-and.pdf [Last Accessed: 30 Nov 2016]

[93] CSO, "Cloud Standards," 2013. [Online]. Available: http://cloud-standards.org/ [Last Accessed: 30 Nov 2016]

[94] Crown, "Data Protection Act 1998," 1998. [Online]. Available: http://www.legislation.gov.uk/ukpga/1998/29/contents [Last Accessed: 30 Nov 2016]

[95] DMTF, “Distributed Management Task Force: Standards and Technology,” 2014. [Online]. Available: http://www.dmtf.org/standards [Last Accessed: 30 Nov 2016]

[96] ETSI, “European Telecommunications Standards Institute,” pp. 1–2, 2014. [Online]. Available: http://www.etsi.org/ [Last Accessed: 30 Nov 2016]

[97] FedRamp, “FedRamp,” 2014. [Online]. Available: http://cloud.cio.gov/fedramp [Last Accessed: 30 Nov 2016]

[98] AICPA, “Generally Accepted Privacy Principles,” 2014. [Online]. Available: https://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/GenerallyAcceptedPrivacyPrinciples/Pages/default.aspx [Last Accessed: 30 Nov 2016]

[99] GICTF, “Global Inter-Cloud Technology Forum,” 2012. [Online]. Available: http://www.gictf.jp/index_e.html [Last Accessed: 30 Nov 2016]

[100] P. Law, “Health Insurance Portability and Accountability Act of 1996,” pp. 1936–2103, 1996. [Online]. Available: http://www.hhs.gov/ocr/privacy/ [Last Accessed: 30 Nov 2016]

[101] R. F. Mills, G. L. Peterson, and M. R. Grimaila, “Measuring Cyber Security and Information Assurance,” Tech. Rep., apr 2009. [Online]. Available: http://www.scopus.com/inward/record.url?eid=2-s2.0-70350638023\&partnerID=tZOtx3y1 [Last Accessed: 30 Nov 2016]

[102] ISAE, “ISAE 3402,” ISAE, Tech. Rep. [Online]. Available: http://www.ifac.org/sites/default/files/downloads/b014-2010-iaasb-handbook-isae-3402.pdf [Last Accessed: 30 Nov 2016]

[103] ISO, “ISO/IEC 27000:2009,” 2014. [Online]. Available: www.iso.org [Last Accessed: 30 Nov 2016]

[104] ITIL, “Information Technology Infrastructure Library,” Axelos, Tech. Rep., 2013. [Online]. Available: www.axelos.com/best-practice-solutions/itil [Last Accessed: 30 Nov 2016]

[105] R. Bank, “ITU - Telecommunication Standardization Sector,” pp. 8 – 12, 2001. [Online]. Available: http://www.itu.int/en/ITU-T/publications/Pages/default.aspx [Last Accessed: 30 Nov 2016]

[106] Jericho Forum, “The Jericho Forum,” Tech. Rep., 2011. [Online]. Available: http://www.opengroup.org/jericho/ [Last Accessed: 30 Nov 2016]

[107] NIST, “Security and Privacy Controls for Federal Information Systems and Organizations Security and Privacy Controls for Federal Information Systems and Organizations,” Natioinal Institute of Standards and Technology, Gaithersburg, MD, Tech. Rep. February, 2014. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf [Last Accessed: 30 Nov 2016]

[108] NERC, “NERC Reliability Standards,” NERC, Tech. Rep. [Online]. Available: http://www.nerc.com/Pages/default.aspx [Last Accessed: 30 Nov 2016]

[109] OASIS, “Organization for the Advancement of Structured Information Standards,” 2014. [Online]. Available: https://www.oasis-open.org/standards [Last Accessed: 30 Nov 2016]

[110] OCC, “OCC - Open Cloud Consortium,” 2011. [Online]. Available: http://opencloudconsortium.org [Last Accessed: 30 Nov 2016]

[111] A. Sill, “Open Grid Forum,” Tech. Rep., 2011. [Online]. Available: https://www.ogf.org/ogf/doku.php/standards/standards [Last Accessed: 30 Nov 2016]

[112] OMG, “Object Management Group,” pp. 1–36, 2003. [Online]. Available: http://www.cloud-council.org/ [Last Accessed: 30 Nov 2016]

[113] PCI Security Standards Council LLC, “Data Security Standard: Requirements and Security Assessment Procedures,” PCI Security Standards Council, Tech. Rep. November, 2013.

[114] SNIA, “Cloud data management interface,” Tech. Rep., 2010.

[115] TOG, “The Open Group,” Tech. Rep., 2014. [Online]. Available: http://www.opengroup.org/ [Last Accessed: 30 Nov 2016]

[116] TM Forum, “TM Forum Frameworx,” The TM Forum, Tech. Rep., 2014. [Online]. Available: http://www.tmforum.org/Frameworx/1911/home.html [Last Accessed: 30 Nov 2016]

[117] M. Vouk, “Cloud Computing Issues, Research and Implementations,” *ITI 2008 - 30th Int. Conf. Inf. Technol. Interfaces*, vol. 16, no. 4, pp. 235–246, 2008.

[118] 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 Comput. Grids Supercomput. - MTAGS ’09*, pp. 1–10, 2009.

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

[120] 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.

[121] S. Pearson and A. Benameur, “Privacy, Security and Trust Issues Arising from Cloud Computing,” in *2010 IEEE Second Int. Conf. Cloud Comput. Technol. Sci.*, no. December. Ieee, nov 2010, pp. 693–702.

[122] C. Wang, Q. Wang, K. Ren, and W. Lou, “Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing,” in *IEEE INFOCOM 2010*, vol. 62, no. 2, 2010, pp. 362–375.

[123] S. Srinivasamurthy, F. Wayne, and D. Q. Liu, “Security and Privacy in Cloud Computing : A Survey Security and Privacy in Cloud Computing :,” in *2010 Sixth Int. Conf. Semant. Knowl. Grids*, vol. 2, 2013, pp. 126–149.

[124] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, “A View of Cloud Computing,” *Commun. ACM*, vol. 53, no. 4, pp. 50—-58, 2010.

[125] S. Ramgovind, M. M. Eloff, and E. Smith, “The management of security in cloud computing,” in *Proc. 2010 Inf. Secur. South Africa Conf. ISSA 2010*, 2010, pp. 1–7.

[126] B. Grobauer, T. Walloschek, and E. Stocker, “Understanding Cloud Computing Vulnerabilities,” *IEEE Secur. Priv.*, vol. 9, no. 2, pp. 50–57, 2011.

[127] F. Doelitzscher, C. Fischer, D. Moskal, C. Reich, M. Knahl, and N. Clarke, “Validating Cloud Infrastructure Changes By Cloud Audits,” in *Proc. - 2012 IEEE 8th World Congr. Serv. Serv. 2012*, 2012, pp. 377–384.

[128] M. L. Hale and R. Gamble, “SecAgreement: Advancing Security Risk Calculations in Cloud Services,” in *Proc. - 2012 IEEE 8th World Congr. Serv. Serv. 2012*, 2012, pp. 133–140.

[129] 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. [Online]. Available: http://hdl.handle.net/10022/AC:P:12821 [Last Accessed: 30 Nov 2016]

[130] 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.

[131] F. Doelitzscher, M. Knahl, C. Reich, and N. Clarke, “Anomaly Detection In IaaS Clouds,” in *Proc. Int. Conf. Cloud Comput. Technol. Sci. CloudCom*, vol. 1, 2013, pp. 387–394.

[132] F. Doelitzscher, T. Ruebsamen, T. Karbe, M. Knahl, C. Reich, and N. Clarke, “Sun Behind Clouds - On Automatic Cloud Security Audits and a Cloud Audit Policy Language,” *… J. Adv. …*, vol. 6, no. 1, pp. 1–16, 2013.

[133] S. Thorpe, T. Grandison, A. Campbell, J. Williams, K. Burrell, and I. Ray, “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.

[134] 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, pp. 362–375, 2013.

[135] J. M. Lopez, T. Ruebsamen, and D. Westhoff, “Privacy-Friendly Cloud Audits with Somewhat Homomorphic and Searchable Encryption,” in *14th Int. Conf. Innov. Community Serv. ”Technologies Everyone”, I4CS 2014 - Conf. Proc.*, 2014, pp. 95–103.

[136] A. S. Sendi and M. Cheriet, “Cloud Computing: A Risk Assessment Model,” *2014 IEEE Int. Conf. Cloud Eng.*, pp. 147–152, 2014.

[137] K. Xiong and X. Chen, “Ensuring Cloud Service Guarantees Via Service Level Agreement (SLA) -based Resource Allocation,” in *Distrib. Comput. Syst. Work. (ICDCSW), 2015 IEEE 35th Int. Conf.* IEEE, 2015, pp. 35–41.

[138] OED, “Oxford English Dictionary,” 1989. [Online]. Available: www.oed.com [Last Accessed: 30 Nov 2016]

[139] B. Guttman and E. A. Roback, “Computer Security,” NIST, Tech.

Rep. 800, 2011. [Online]. Available: http://books.google.com/books?id=KTYxTfyjiOQC\&pgis=1 [Last Accessed: 30 Nov 2016]

[140] J. A. Chaula, "A Socio-Technical Analysis of Information Systems Security Assurance: A Case Study for Effective Assurance," Ph.D. dissertation, 2006. [Online]. Available: http://scholar.google.com/scholar?hl=en\&btnG=Search\&q=intitle:A+Socio-Technical+Analysis+of+Information+Systems+Security+Assurance+A+Case+Study+for+Effective+Assurance\#1 [Last Accessed: 30 Nov 2016]

[141] R. K. L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, and B. S. Lee, "TrustCloud: A framework for accountability and trust in cloud computing," *Proc. - 2011 IEEE World Congr. Serv. Serv. 2011*, pp. 584–588, 2011.

[142] 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, pp. 3–44.

[143] EU, "Unleashing the Potential of Cloud Computing in Europe," 2012. [Online]. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SWD:2012:0271:FIN:EN:PDF [Last Accessed: 30 Nov 2016]

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

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

[146] D. Catteddu and G. Hogben, Cloud Computing: Benefits, Risks and Recommendations for Information Security, Computing, Vol. 72, no. 1, pp. 20092013, 2009.

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

[148] OWASP, "OWASP Top Ten Vulnerabilities 2013," 2013. [Online]. Available: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project [Last Accessed: 30 Nov 2016]

[149] OWASP, "OWASP SQL Injection Cheat Sheet," 2016. [Online]. Available: https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet [Last Accessed: 30 Nov 2016]

[150] OWASP, "OWASP Injection Prevention Cheat Sheet," 2016. [Online]. Available: https://www.owasp.org/index.php/Injection_Prevention_Cheat_Sheet [Last Accessed: 30 Nov 2016]

[151] OWASP, "OWASP LDAP Injection Prevention Cheat Sheet," 2016. [Online]. Available: https://www.owasp.org/index.php/LDAP_Injection_Prevention_Cheat_Sheet [Last Accessed: 30 Nov 2016]