Reflecting on Whether Checklists Can Tick the Box for Cloud Security.

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*—All Cloud computing standards are dependent upon checklist methodology to implement and then audit the alignment of a company or an operation with the standards that have been set. An investigation of the use of checklists in other academic areas has shown there to be significant weaknesses in the checklist solution to both implementation and audit; these weaknesses will only be exacerbated by the fast-changing and developing nature of clouds. We examine the problems that are inherent with using checklists and seek to identify some mitigating strategies that might be adopted to improve their efficacy.**

***Keywords*—security; standards; compliance; assurance; audit**

I. Introduction

Standards have the checklist as an implementation and audit feature embedded in their very essence. Checklists are a relatively simple subset of the broader category of "decision aids". Decision aids can also include various modelling techniques and expert systems. Other academic disciplines ranging from accountancy to medicine have critically assessed the value and problems associated with decision aids (see Beck, 2014 [1] for a recent example), whereas the computer science literature has little critical appraisal of the efficacy of the implicit checklists embedded in the security standards. Acceptance of an emphasis on compliance with standards being the aim rather than discovery (or non-discovery) of an actual security issue is a further problem exacerbated by the security environment changing faster than any agreed standard and consequent checklist can keep up with. This paper seeks to question checklist efficacy and, by seeking questions and mitigating practices from other disciplines, to inform a more developed and less naïve discussion of such decision aids within cloud computer security protocols and audits.

The remainder of the paper is organized as follows: in Section II we discuss the issues of cloud audit and accountability, and; in Section III the use of checklists in cloud audit; in Section IV we look at checklist use in wider society; in Section V we consider whether they work, and ask how they might be made better; and in Section VI our conclusions.

II. Audit and Accountability in the Cloud

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 useful background on this issue. Cloud computing audit, by comparison, can not be considered a mature field, and there will clearly be some way to go before it will be able to catch up with work done in the accounting profession. An obvious area of weakness arises when taking audit professionals from the accounting world out from their comfort zone, and placing them in a more technical field. Equally, the use of people with a computing background can help some of these issues, but in turn, their lack of audit background presents another weakness.

Some research into cloud audit has been undertaken, but has been limited due to a combination of the lack of maturity in this field and the greater technical complexities posed by cloud computing. A number of potential issues [3] arise with the adoption of cloud computing, including security, privacy and audit. Foster et al [4] compare and contrast cloud computing with grid computing and comment on how the important issues have changed. A proposed framework for promoting trust in the use of cloud systems [5] identified the need to ensure a proper audit trail is maintained. Companies will be unable to pass audit by their customers [6] if they are unable to demonstrate an adequate level of control over cloud data. Wang et al [7] propose a mechanism to allow a third party auditor to conduct a cloud audit on behalf of a customer who may not have the skills to carry it out themselves. Chow et al [8] consider some implications of the difficulties of cloud audit and Armbrust et al [9] note that lack of auditability of cloud presents the no. 3 barrier to cloud take-up. Pearson and Charlesworth [10] consider the development of procedural and technical solutions to address jurisdictional privacy and security risks within the cloud, proposing that procedural and technical solutions are co-designed to demonstrate accountability as a path forward to resolving jurisdictional privacy and security risks within the cloud.

While many of the issues surrounding cloud computing are very similar to previous issues [11], two facets are to some degree new and fundamental to cloud computing: the complexities of multi-party trust considerations; and the ensuing need for mutual auditability. The lack of auditability[12], particularly in light of the stringent requirements of the Sarbanes Oxley Act, is the no. 3 barrier to cloud adoption. Pearson and Benameur [13] consider the use of tracing audit authorities to enhance privacy, security and trust. Ramgovind et al [14] provide an overall security perspective of Cloud computing and aim to highlight the security concerns that should be properly addressed and managed to realize its full potential. Zhou et al [15] propose an additional audit layer to be run on the cloud system to "watch over" what goes on in the cloud. Wang et al [16] propose a scheme to support scalable and efficient public

auditing in cloud computing, noting the challenge in trying to provide adequate public audit, while preserving privacy.

A proposed Accountability as a Service approach [17] using continuous cloud monitoring and audit to ensure better quality of service, uses a novel design to achieve Trustworthy Service Oriented Architecture (TSOA) in the Cloud through enforcing strong accountability. Cloud services should be mutually accountable to both cloud service provider and customer [18], to ensure proper service levels can be achieved, but some challenges remain to be overcome. Despite auditability being one of the key components of trust [19], most of the prominent cloud service providers are failing to address this. They suggest that users can at best monitor the virtual hardware performance metrics and the system event logs of the services they engage and that service providers could increase accountability and auditability by using mechanisms such as tracking of file access histories, which will empower service providers and users to reduce many of the key threats.

Proper metrics are not yet adapted to cloud infrastructures [20] and there are no standardized cloud-specific security metrics that customers can use to monitor the security status of their cloud resources. Until such standard security metrics are developed and implemented, controls for security assessment, audit, and accountability will be more difficult and costly and might even be impossible to employ. A novel highly decentralized information accountability framework [21] to keep track of the actual usage of the users' data in the cloud is mooted. Pearson et al [22] propose a data management solution to provide accountability within the cloud as well as addressing privacy issues, using trust authorities. Cloud and IT service providers should act as responsible stewards [23] for the data of their customers and users, but note the absence of accountability frameworks for distributed IT services makes it difficult for users to understand, influence and determine how their service providers honour their obligations. The threat posed by the lack of proper auditability in the cloud is recognised [24], particularly where multiple cloud service providers are involved in a single provision to a customer. Ruebsamen and Reich [25] consider the use of audit agents in the cloud to try to address this issue. Doelitzscher et al [26] begin experimenting with the use of neural networks in cloud systems to detect anomalies, specifically in IaaS clouds. While this has proved successful utilising historic data, it is not yet sufficiently developed to run in a real time environment, but offers some promise. We can see that concerns are being expressed in cloud audit and accountability research. Meanwhile, audit, accountability and compliance with standards continue to be practised utilising more basic techniques as we will see in the next section.

III. Checklists in the Cloud

Cloud security is often approached through standards compliance, with a number of security standards already evolved over recent years, but the very number presents a weakness, namely which one to comply with. Should it be ARTS, CSA, CSCC, DMTF, ENISA, ETSI, FedRamp, GAPP, GICTF, ISO, ITU, NIST, OASIS, OCC, OGF, OMG, PCI or SNIA ([27]–[31]), to name but a few? None of these standards provides complete security — there is no "one size covers all" — another weakness. Even compliance with all standards will not guarantee complete security, yet another weakness.

Many standards were developed before cloud computing evolved. The pace of evolution of new technology far outstrips the capability of standards organizations to keep up with the changes [32], leading to further weakness — the lack of currency. There is a commendable move between standards organizations to chart common ground between their respective standards, but there is a long way to go. The standards tend to be described in a hierarchical fashion, resulting in what is essentially a structured list of areas to be addressed. The implementation process involves audit by an external body, accredited by the standards organization, who must demonstrate a high level of expertise in carrying out audit work, have a sufficient level of experience and a good understanding of the requirements of the standard. Usually many of these audit firms come from the accounting profession, but this is not always the case. One factor common to all is that due to economic considerations, the full audit is unlikely to be carried out by the designated audit professional. Work is delegated to junior, less experienced, staff and is frequently implemented by the use of checklists. The list of areas of the standard to be addressed lends itself to the use of checklists, and many standards organizations encourage this approach. However, the checklist will only ever be as good as the expert who devises the questions to be asked within the checklist.

This obsession with the checklist approach spawns further weaknesses. The company implementing the standard is seeking to be compliant, thus will gear their systems to meet the requirements of the standard, but as a result may take their eye off the ball regarding more basic monitoring controls, presenting a weakness. The auditors seek to ensure the areas to be addressed in the standard are addressed by the company, and will do likewise, with the focus on completing the checklist leading to acquiring a sufficient number of checks in the "Yes" boxes. There is another weakness to be considered — the fact that compliance, once obtained, is not necessarily repeated with any degree of regularity. There is only a requirement to seek re-certification following major system change, or a few years down the line. A further weakness concerns the nature of the questions which are actually asked. Here are a couple of examples which clearly demonstrate whether the right question is being asked, but without sufficient depth to be able to gauge the degree of success of the outcome:

Q Are suitable controls applied when personnel use your equipment to work at home? **Yes No N/A**

A A Yes answer is not enough. There is a need to understand how effective the controls are in operation. If the company applies suitable controls, they get compliance, but if the controls don't work, they don't get security!

Q Are your information classification guidelines consistent with your access control policy? **Yes No N/A**

A Again, a Yes answer is not enough. There is a need to understand how well the underlying dependency on the access control policy will work in practice. If company guidelines are consistent, but underlying controls are flawed, there is compliance, but if the controls don't work, there is no security! Similarly, if the information classification guidelines are

consistent with the underlying access control policy, but the guidelines are ignored, there is compliance, but no security.

While this results in compliance, where is the value in compliance with a standard which does not cover everything, is not current, and not necessarily asking the right kind of questions, let alone often enough? So, are checklists all bad news? Not necessarily. There are a number of advantages. Providing they have been properly devised by a suitable expert, their use can be substantially delegated to less skilled, i.e. cheaper staff. They can be completed relatively quickly and are particularly well suited to repetitive tasks. Providing sufficient supporting evidence is collected to substantiate the answers given, this can provide the basis for an excellent working paper for both internal and external audit review purposes.

This has to be considered in the light of changes in the threat environment. Latest estimates [33] are that over 200,000 new pieces of malware are released globally every day, which represents over 73 million new annual global threats potentially deployable against every computer connected to the internet. How can standards compliance be reconciled with this rapidly evolving threat environment, which is evolving far faster than the standards can keep up? This disparity between what protection companies believe they have and the real world presents a clear and present danger. Research into this area within cloud computing is somewhat sparse. Chen and Yoon [11] and Bhandari and Mishra [34] use checklists at a high level of abstraction in considering cloud audit, but neither attempt to consider the implications of their use at a detailed technical level. Perhaps we may gain some insight by looking at how checklists are used in other areas of society. Their use in areas such as audit, medicine, aviation, education and a variety of other areas present a reasonably mature field of research to review.

IV. Checklists in Wider Society

Many academic disciplines consider the use of checklists within their own area and do so critically, highlighting likely areas of weakness. Before examining two specific disciplines in more detail, we endeavour to give an impression of the broad spread of interest and concern across academia. Colmar [35] considered the limitations of checklists in assessing child behaviour and academic achievement, concluding that they have "real limitations", and Hosie [36] notes that checklists need to be tailored to the type of course (online in this case) being evaluated. Palmer [37] looks specifically at well known aviation flight checklists and considers the impact of the automation of checklists and how that lead to reduced awareness of the situation and of the system itself. Indeed, in their field study, Degani and Wiener [38] report the lack of attention to human factors and improper use can impact adversely on safety. Cooperative evaluation [39] is most useful for early feedback about re-design in a rapid iterative cycle in the context of software development. This can be used with:

- an existing product that is to be improved or extended;
- with an early partial prototype or simulation;
- with a full working prototype.

In a survey of 117 checklists from 24 sources [40], different categories of checklist items are discussed and examples are provided of good items as well as those that should be avoided, which highlights the need for feedback on checklist effectiveness. There are some very interesting observations on the logic behind [41], and the various methodologies employed in, differing types of evaluation checklist providing some ideas for good design. In trying to improve project estimation [42] found that checklists could improve estimation accuracy, reducing over-runs. Poor or even deceitful use of checklists in the food chain [43] has clear and obvious warning bells for cloud security with its multiple players, complex structures and potentially differing priorities of each of the participant individuals or companies, and emphasises the need for checklist governance. We now move on to consider the two specific disciplines in more detail, starting with medicine.

A. Checklists in Medicine

The use of decision aids and checklists is an important topic as they appear to offer better healthcare, being available more widely and potentially at lower cost, yet recognising that if they do not work, medical outcomes could be catastrophic. Medical studies are also aware of broader societal use of checklists [44], and see that concerns over stress and tiredness when using checklists in a medical situation would be mirrored in other settings. Most studies are positive about checklist use but stipulate some limiting factors or additional elements that would facilitate their usefulness. Testing, careful design and training for users, are accepted as useful [45], offering *"reliable repeatable outcomes."*There is a need for a qualitative judgement on the outcome of a checklist[46] by a *"carefully composed multi-disciplinary group"*(p336). Some more recent studies — Bosk et al [47], Winters et al [48], Davidoff [49] and Nanji and Cooper [50] — are also positive in principle about the use of checklists whilst stating some additional requirements for a successful checklist. Bosk [47] tries to reduce the excitement of seeing checklists as a universal panacea, stating the need for assessing outcomes and for them to be used in an appropriate performance culture. Winters et al [48] put forward arguments for broader use of checklists to spread knowledge more widely.

Checklists can be game-changing [49], yet, their use *"as quick and simple tools aimed to buttress the memory and skills of expert professionals"*(p207), seemingly does not see them as spreading an expert's knowledge to become more widely applied by those with lesser knowledge or professional training. There is a need for careful design and training [50] whilst also being positive about the value of checklists. Some concerning negative results also exist. Regehr et al[51], find that a global ranking scale, allowing for an expert to use their broader expertise, significantly outscored checklists. In a similar vein, Hodges et al [52], found that clerks outscored consultants with a checklist, but the consultants were the best performers when allowed a broader ranking approach. With this ongoing level of interest, a survey of checklist medical research literature found [53] that *"a highly effective, standardized methodology for the development and design of medical-specific checklists has not previously been developed and validated, which has likely contributed to their inconsistent use in several key fields of medicine, despite evidence of their fundamental role in error management"*(p22). Hence one might conclude that the medical literature sees checklists as helpful with caveats and limitations, though has yet to find a bullet-proof approach for their development, design or, implementation. The second

example discipline, which perhaps has a more relevant bearing on cloud computing, is audit.

B. Checklists in Audit

The auditing of financial statements is a further area where there has been an increasing reliance on checklists and other decision aids. A particular focus has been on the assessing of fraud risk, which would have some similarities to detecting security breaches in the cloud. The following paragraphs give a flavour of the research. Comparing the outcomes of unaided decisions [54] when checklists, logit models or expert systems are used, the expert system outperformed, with logit model also out-performing checklists. Dowling [55] concluded that the appropriate use of a checklist depended on corporate pressures, auditor attitude and the auditor's position in the firm hierarchy.

In fraud detection [56] noted the poor uptake of approaches that had a good pedigree of problem finding — including discovery sampling, data mining, forensic accounting and digital analysis software. They question the quality of the cost-benefit trade-off decisions that were being made especially by small firms who might see the additional cost as prohibitive, but don't fully assess the potential costs of undiscovered fraud. Boritz and Timoshenko [57], which we will return to later, try and map out the issues that need to be addressed in making the use of a checklist more robust in delivering broad objectives (as opposed to answering a myriad of subsidiary questions). They present their concerns in a diagram that we generalize and adapt below. Auditors who used a standard risk checklist [58], structured by SAS 82 (an AICPA audit standard) risk categories, made lower risk assessments than those without a checklist, which suggests that the use of the checklist was associated with a less effective diagnosis of the fraud and found that poorly designed checklists had the potential of stopping an auditor from forming a good overall picture of the fraud situation. Mock and Turner [59], using a sample of 202 audit clients obtained from three large audit firms, found evidence that following the issuance of SAS No. 82, audits became less reliant on the outcomes of checklists.

One common checklist in the audit of financial statements is a check that all disclosures required by current accounting standards have been included in the report to be published to shareholders. Rinsum [60] discusses the problem that this technical achievement (i.e. conformity) to the standards does not necessarily lead to the broader (and in theory more important) achievement of delivering a meaningful and reasonable view and understanding of the company's financial position. Checklists, it seems might be useful for assessing minute item-by-item compliance, but risk undermining the development of the bigger picture. This might also be seen as a good example of a checklist making life easier for the auditing company whilst potentially short changing the ultimate client — the shareholder. Both of these points can be seen to have direct relevance to a cloud security checklist.

V. Do Checklists Work?

This leads us to the obvious question, do checklists work? On the evidence of our discussion, there is clearly no definitive answer to that question. Sometimes they do, sometimes they don't and sometimes they might if a few changes were to be made. Let us examine why this might be.

On the plus side:

- we have the possibility of using less senior staff;
- we have the possibility of saving time, and money;
- checklists are ideally suited to repetitive tasks;
- providing sufficient supporting evidence is collected, the checklist approach can work well.

On the minus side:

- multiplicity, lack of coherence, lack of completeness, currency of current standards and lack of frequency of the audit are issues;
- slavish following of checklist questions to detailed structure of standards;
- can lead to company taking eye off the ball, missing the basics;
- can lead auditors to focus on the standards checklist rather than on the underlying issues;
- the type of questions asked are often not searching enough.

Having recognised the inherent failings of the checklist, we need to consider how we might go about improving this situation. We return to Boritz and Timoshenko [61], who produced an interesting diagram to characterise factors which might be incorporated to improve the effectiveness of the checklist.

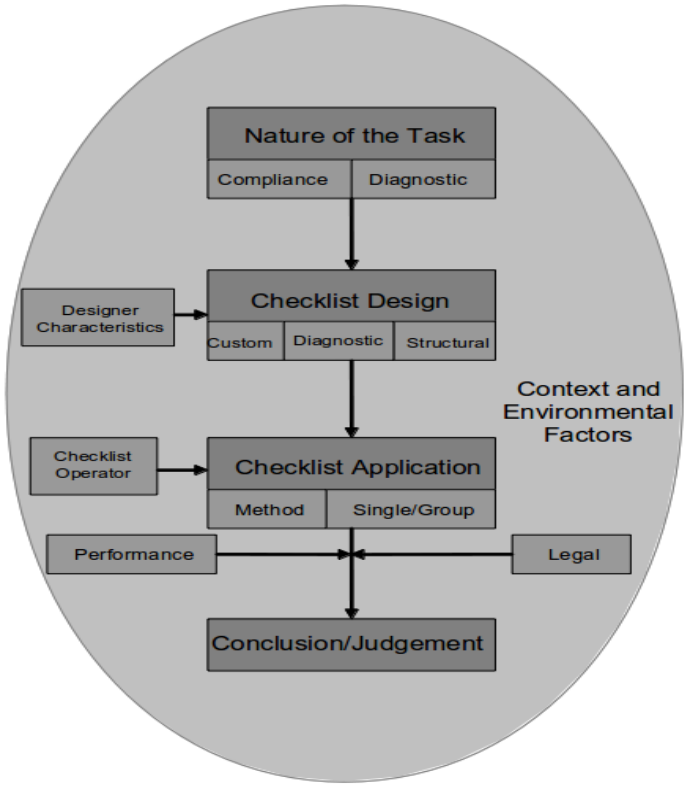

Fig. 1. Factors Affecting the Effectiveness of a Checklist Flowchart Adapted from Boritz and Timoshenko [61]

We have adapted this diagram to suit the particular needs of cloud computing. For each question included in a checklist, we must consider the context in which it will apply, taking into

account any appropriate environmental factors. There will need to be at the start point, a firm idea of the nature of the task, and at the end point, an expectation of what the desired outcome should be. We look at each of the stages in turn. Starting with the nature of the task, we can categorise that into either a compliance-based task, or a diagnostic-based task. Depending on which category is appropriate, the type of question needed will vary, e.g. we may have a compliance requirement which we are hoping to demonstrate compliance with, but before we can demonstrate compliance, we may have to undertake some diagnostic work to provide the necessary assurance that the requisite level of compliance has been achieved.

This takes us to the next stage, the checklist design. This will be heavily influenced by the checklist designer characteristics. The degree to which a successful design is achieved by an auditor who is to design the checklist will very much depend on their experience, expertise and whether they are prone to overconfidence. The checklist design will comprise three categories: custom; diagnostic and structural. In the custom section, the degree to which a generic approach, or a customized approach is required will influence the design. In the diagnostic section, will the approach need to broad, or a narrow array of items only and will predictive strength of items need to be considered? In the Structure section, will the checklist have a hierarchical organization? Will there need to be decomposition into categories and sub-categories?

This, leads to the next stage, the checklist application. This will be heavily influenced by the checklist operator. As with the checklist designer, their background experience, expertise and the degree of overconfidence they might exhibit will all have an impact on the successful outcome of the exercise. The checklist application stage will be broken down into method, and single/group sections. The method of combining cues will need to consider whether the approach should be subjective/intuitive, or deliberative, or model based (regression, expert system, etc). The single/group section will need to consider whether the audit is being conducted by an interactive audit team, or by a non-interactive audit team, or by an individual auditor.

There will be other factors influencing the checklist application. Performance issues such as financial incentives, justification, outcome feedback, and so on may have to be taken into account. On the legal front, there are legal liability considerations, such as will the result be defend-able in court? This should allow reaching the conclusion/judgement stage. By properly taking all the previous influences into account, it will be possible to reach a satisfactory conclusion, or judgement, or some other result, that will more accurately reflect the realities of the situation under review. It is important that practitioners do not lose sight of the overview when using checklists and they must be fully aware of the shortcomings outlined earlier, and take them fully into account when carrying out their work. They should not be blinded by the use of checklists to the point where the checklist becomes the focus of the audit. Rather, the checklist should always be viewed as a very useful tool in the auditor's armoury.

VI. Conclusion

In this short paper, we have attempted to present some of the complexities and issues around the use of decision aids and checklists in particular. Other areas of academic study have a more developed critique of checklists than computer science and cloud security in particular, although it is clear that lessons from these areas are of relevance to the cloud. It would seem that there is no one approach or system that can confidently be applied to checklist design, implementation and interpretation to guarantee meaningful, robust and trustworthy results. We have shown some pointers to improving current practice and to the likelihood that checklists and their use will always be flawed, but always tempting due to the potential for low cost mass implementation. A checklist may only be able to check for conformity to a standard (in cloud, an inevitably out of date standard) rather than guarantee the absence of (or finding of) underlying problems.

The checklist straight jacket may also deny an experienced practitioner the opportunity to develop a rounded understanding of the situation by being forced to focus on the individual trees rather than the wood as a whole. Other approaches to addressing conformity and audit from other disciplines could be usefully considered in a cloud setting. These alternatives to checklists would be likely to have the downside of greater cost, but the potential upside of greater benefit.

References

[1] G. M. Beck, R. Limor, and P. R. Wheeler, "The Effect of Changes in Decision Aid Bias on Learning: Evidence of Functional Fixation," *J. Inf. Syst.*, vol. 28, no. 1, pp. 19–42, 2014.

[2] B. Duncan and M. Whittington, "Compliance with Standards, Assurance and Audit: Does this Equal Security?" in *SIN2014*, Glasgow, 2014.

[3] M. A. Vouk, "Cloud Computing Issues , Research and Implementations," *J. Comp. Inf. Tech.*, vol. 16, no. 4, pp. 235–246, 2008.

[4] I. Foster, Y. Zhao, I. Raicu, and S. Lu, "Cloud Computing and Grid Computing 360-degree compared," in *Grid Comp. Envirn. Work. GCE 2008*, 2008, pp. 1–10.

[5] D. Bernstein, S. Diamond, and M. Morrow, "Blueprint for the Intercloud Protocols and Formats for Cloud Computing Interoperability," in *Int Web App. Serv. 2009. ICIW'09. 4th Int. Conf.*, 2009, pp. 328–336.

[6] N. Leavitt, "Is Cloud Computing Really Ready for Prime Time?" *Computer (Lng. Bch. Calif).*, vol. 42, no. Jan, pp. 15–20, 2009.

[7] S. C. Wang, K. Q. Yan, S. S. Wang, and C. P. Huang, "Achieving high efficient agreement with malicious faulty nodes on a cloud computing environment," *Proc. 2nd Int. Conf. Intact. Sci. Inf. Tech. Cult. Hum. - ICIS '09*, pp. 468–473, 2009.

[8] 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 Comp. Secur.*, 2009, pp. 85–90.

[9] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the Clouds: A Berkeley View of Cloud Computing," *Science (80-.).*, vol. 53, no. UCB/EECS-2009-28, pp. 07–013, 2009.

[10] S. Pearson and A. Charlesworth, "Accountability as a Way Forward for Privacy Protection in the Cloud," *Computing*, no. December, pp. 1–15, 2009.

[11] Y. Chen and R. Sion, "On Securing Untrusted Clouds with Cryptography," *Science (80-.).*, pp. 109–114, 2010.

[12] B. Armbrust, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, and A. Rabkin, "A View of Cloud Computing," *Comm. ACM*, vol. 53, no. 4, pp. 50—-58, 2010.

[13] S. Pearson and A. Benameur, "Privacy, Security and Trust Issues Arising from Cloud," in *2nd IEEE Int. Conf. Cloud Comp. Tech. Sci. CloudCom 2010*, no. Dec, 2010, pp. 693—-702.

[14] S. Ramgovind, E. Mm, and E. Smith, "The Management of Security in Cloud Computing," in *Inf. Sec. Sth Africa (ISSA), 2010*, 2010, pp. 1–7.

[15] M. Zhou, R. Zhang, W. Xie, W. Qian, and A. Zhou, "Security and privacy in cloud computing: A survey," in *Proc. - 6th Int. Conf. Semant. Knowl. Grid, SKG 2010*, 2010, pp. 105–112.

[16] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," in *IEEE INFOCOM 2010. Priv-Pres*, 2010, pp. 1–9.

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

[18] A. Haeberlen, "A Case for the Accountable Cloud," *ACM SIGOPS Oper. Syst. Rev.*, vol. 44, no. 2, pp. 52–57, 2010.

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

[20] B. Grobauer, T. Walloschek, and E. Stocker, "Understanding Cloud Computing Vulnerabilities," *Secur. privacy, IEEE*, vol. 9, no. April, pp. 50–57, 2011.

[21] A. Squicciarini, S. Sundareswaran, D. Lin, and S. Huang, "Promoting Distributed Accountability in the Cloud," in *IEEE 4th Int. Conf. Cloud Comp. Prom.*, 2011, pp. 113–120.

[22] S. Pearson, M. C. Mont, and G. Kounga, "Enhancing Accountability in the Cloud via Sticky Policies," in *Sec. Trust Comp. Data Mgt. App.*, 2011, pp. 146–155.

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

[24] M. Theoharidou, N. Papanikolaou, S. Pearson, and D. Gritzalis, "Privacy Risk, Security, Accountability in the Cloud," in *2013 IEEE 5th Int. Conf. Cloud Comput. Technol. Sci.*, 2013, pp. 177–184. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6753795

[25] T. Ruebsamen and C. Reich, "Supporting Cloud Accountability by Collecting Evidence Using Audit Agents," in *CloudCom 2013*, 2013, pp. 185–190.

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

[27] CSO, "Cloud Standards," 2013. [Online]. Available: http://cloud-standards.org/

[28] ENISA, "A Security Analysis of Next Generation Web Standards," 2013. [Online]. Available: http://www.enisa.europa.eu/

[29] CSA, "Security Guidance for Critical Areas of Focus in Cloud," Cloud Security Alliance, Tech. Rep., 2012.

[30] T. F. R. Program and A. Management, "FedRamp," 2014. [Online]. Available: http://cloud.cio.gov/fedramp

[31] P. S. S. Council, "Data Security Standard Requirements and Security Assessment Procedures," PCI Security Standards Council, Tech. Rep. Nov, 2013.

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

[33] Kaspersky, "Global Corporate IT Security Risks : 2013," Tech. Rep. May, 2013. [Online]. Available: http://media.kaspersky.com/en/business-security/Kaspersky_Global_IT_Security_Risks_Survey_report_Eng_final.pdf

[34] R. R. Bhandari and N. Mishra, "Encrypted IT Auditing and Log Management on Cloud Computing," *J. Comp. Sci.*, vol. 8, no. 5, pp. 302–305, 2011.

[35] S. Colmar, "A perspective on behaviour checklists," *Educ. Psychol.*, vol. 8, no. 1-2, pp. 117–121, 1988.

[36] P. Hosie, R. Schibeci, and A. Backhaus, "A framework and checklists for evaluating online learning in higher education," *Assess. Eval. High. Edu.*, vol. 30, no. 5, pp. 539–553, 2005.

[37] E. Palmer and A. Degani, "Electronic checklists: Evaluation of two levels of automation," in *Proc. Sixth Symp. Aviat. Psychol.*, 1991, pp. 178–183.

[38] A. Degani and E. L. Wiener, "Cockpit checklists: Concepts, design, and use," *Hum. Factrs J. Hum. Factrs Ergon. Soc.*, vol. 35, no. 2, pp. 345–359, 1993.

[39] A. Monk, L. Davenport, J. Haber, and P. Wright, *Cooperative Evaluation: A run-time guide - Appendix 1*. Prentice Hall London, 1993.

[40] B. Brykczynski, "A survey of software inspection checklists," *ACM SIGSOFT Softw. Eng. Notes*, vol. 24, no. 1, p. 82, 1999.

[41] M. Scriven, "The logic and methodology of checklists," *Methodology*, vol. 23, no. Oct, pp. 280–288, 2000.

[42] K. M. Furulund and K. Molokken-Ostvold, "Increasing software effort estimation accuracy using experience data, estimation models and checklists," in *Qual. S/ware, 2007. QSIC'07. 7th Int. Conf.* IEEE, 2007, pp. 342–347.

[43] 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.

[44] B. M. Hales and P. J. Pronovost, "The checklista tool for error management and performance improvement," *J. Crit. Care*, vol. 21, no. 3, pp. 231–235, 2006.

[45] S. H. Downs and N. Black, "The feasibility of creating a checklist for the assessment of the methodological quality both of randomised and non-randomised studies of health care interventions." *J. Epid. Comm. Health*, vol. 52, no. 6, pp. 377–384, 1998.

[46] R. Harbour and J. Miller, "A new system for grading recommendations in evidence based guidelines," *Bmj*, vol. 323, no. 7308, pp. 334–336, 2001.

[47] C. L. Bosk, M. Dixon-Woods, C. A. Goeschel, and P. J. Pronovost, "Reality check for checklists," *Lancet*, vol. 374, no. 9688, pp. 444–445, 2009.

[48] B. D. Winters, A. P. Gurses, H. Lehmann, J. B. Sexton, C. J. Rampersad, and P. J. Pronovost, "Clinical review: checklists-translating evidence into practice," *Crit Care*, vol. 13, no. 6, p. 210, 2009.

[49] F. Davidoff, "Checklists and guidelines: imaging techniques for visualizing what to do," *JAMA*, vol. 304, no. 2, pp. 206–207, 2010.

[50] K. C. Nanji and J. B. Cooper, "It is time to use checklists for anesthesia emergencies: Simulation is the vehicle for Testing and Learning," *Reg. Anesth. Pain Med.*, vol. 37, no. 1, pp. 1–2, 2012.

[51] G. Regehr, H. MacRae, R. K. Reznick, and D. Szalay, "Comparing the psychometric properties of checklists and global rating scales for assessing performance on an OSCE-format examination." *Acad. Med.*, vol. 73, no. 9, pp. 993–997, 1998.

[52] B. Hodges, G. Regehr, N. McNaughton, R. Tiberius, and M. Hanson, "OSCE checklists do not capture increasing levels of expertise," *Acad. Med.*, vol. 74, no. 10, pp. 1129–1134, 1999.

[53] B. Hales, M. Terblanche, R. Fowler, and W. Sibbald, "Development of medical checklists for improved quality of patient care," *Int. J. Qual. Heal. Care*, vol. 20, no. 1, pp. 22–30, 2008.

[54] M. M. Eining, D. R. Jones, and J. K. Loebbecke, "Reliance on Decision Aids: An Examination of Auditors' Assessment of Management Fraud," *Audit. A J. Pract. Theory*, vol. 16, no. 2, pp. 1–19, 1997.

[55] C. Dowling, "Appropriate Audit Support System Use: The Influence of Auditor, Audit Team, and Firm Factors," *Acct. Rev.*, vol. 84, no. 3, pp. 771–810, May 2009.

[56] J. L. Bierstaker, R. G. Brody, and C. Pacini, "Accountants' perceptions regarding fraud detection and prevention methods," *Mgt. Audit. J.*, vol. 21, no. 5, pp. 520–535, 2006.

[57] J. E. Boritz and L. Timoshenko, "On The Use Of Checklists In Auditing: A Commentary," *Curr. Issues Audit.*, vol. 8, no. 1, pp. C1 – C25, Feb. 2014.

[58] S. K. Asare, U. Florida, A. Wright, and B. College, "The Effectiveness of Alternative Risk Assessment and Program Planning Tools in a Fraud Setting," *Contp. Acct. Res.*, vol. 21, no. 2, pp. 325 – 352, 2004.

[59] T. J. Mock and J. L. Turner, "Auditor Identification of Fraud Risk Factors and their Impact on Audit Programs," *Int. J. Audit.*, vol. 77, no. 82, pp. 59–77, 2005.

[60] M. van Rinsum, V. S. Maas, and D. Stolker, "Disclosure Checklists and Bias in Audit Judgments," *Available SSRN 2218408*, pp. 1–43, 2013.

[61] J. E. Boritz and L. Timoshenko, "On The Use Of Checklists In Auditing: A Commentary," *Curr. Issues Audit.*, 2014.