The Importance of Proper Measurement for a Cloud Security Assurance Model

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*—Defining proper measures for evaluating the effectiveness of an assurance model, which we have developed to ensure cloud security, is vital to ensure the successful implementation and continued running of the model. We need to understand that with security being such an essential component of business processes, responsibility must lie with the board. The board must be responsible for defining their security posture on all aspects of the model, and therefore must also be responsible for defining what the necessary measures should be. Without measurement, there can be no control. However, it will be also be necessary to properly engage with cloud service providers to achieve a more meaningful degree of security for the cloud user.**

Keywords*—security; privacy; standards; compliance; assurance; audit; measurement; cloud service providers; service level agreements

I. Introduction

Achieving information security in the cloud is not a trivial process. There are a great many challenges to overcome and, with Pym, we addressed some of those in earlier work [1] developing a conceptual model for cloud security assurance, where we addressed three key challenges, namely standards, proposed management method and complexity. In this current work, we consider the importance of defining proper measurement mechanisms to ensure the correct working of the assurance model.

There are, of course, many other issues, and we discuss some of these in Section II, where we look at the definition of security goals, compliance with cloud security standards, audit issues, the impact of management approaches on security, and how complexity and the lack of responsibility and accountability affects cloud security. The remainder of the paper is organized as follows: in Section III we give a brief overview of how our framework operates; in Section IV we discuss how the literature approaches measurement; In Section V we discuss how we might go about developing metrics to measure performance of the security goals of security and privacy. In Section VI we address the remaining key issue to be tackled; and in Section VII we discuss our conclusions.

II. The Challenges

There are a number of challenges which need to be addressed in order to achieve the goal of good security. The fundamental concepts of information security are confidentiality, integrity, and availability (CIA), a concept developed when it was common practice for corporate management to run a company under agency theory. We have all seen how agency theory has failed to curb the excesses of corporate greed. The same is true for cloud security, which would suggest a different approach is needed. We address the following important points in turn: definition of security goals, compliance with cloud security standards, audit issues, the impact of management approaches on security, and how complexity and the lack of responsibility and accountability affects cloud security.

In 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 measures would be required. More emphasis is now being placed on responsibility and accountability [2], social conscience [3], sustainability [4][5], resilience [6] and ethics [7].

Responsibility and accountability are, in effect, mechanisms we can use to help achieve all the other security goals. Since social conscience and ethics are very closely related, we can expand the traditional CIA triad to include sustainability, resilience and ethics. This expansion of security requirements can help address some of the shortcomings of agency theory, but also provides a perfect fit to stewardship theory. Stewardship carries a broader acceptance of responsibility than the self-interest embedded in agency. This breadth extends to acting in the interests of company owners and potentially society and the environment as a whole.

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

The pace of evolution of new technology far outstrips the capability of international standards organisations to keep up with the changes [9], 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.

In [8], we have addressed the question of whether compliance with standards, assurance and audit can provide security,

and in [10], we have addressed one of the fundamental weaknesses of the standards compliance process.

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 [8] 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 work done in the accounting profession.

An obvious area of weakness arises when taking audit professionals from the accounting world out of their comfort zone, and placing them in a more technical field. Equally, the use of people with a computing background can overcome some of these issues, but their lack of audit background presents another weakness. Clearly further research will be needed in this area.

Looking at management approach, we would argue that a shift from agency behaviour to a stewardship approach can go a long way to reducing the major weaknesses inherent in an agency approach to security in cloud ecosystems. We have observed that cloud service providers (CSP)s have developed their cloud business models using agency theory. Pallas et al [11] suggest that agency theory models the current relationship between CSPs and cloud users very well, further suggesting this expresses all the weaknesses of agency and highlights many of the issues still faced today.

Given the potential multiplicity of actors, and the complexities of their relationships with each other in cloud ecosystems, it is clear that simple traditional agency relationships (where each actor looks to their own short term ends) will no longer be able to handle fully the security implications for users of these ecosystems.

There is a clear need for developing a stronger mechanism to ensure users of such ecosystems can be assured of the security of their information. In [12], we addressed the cloud security issue with management method, and argue that the historic reliance on agency theory to run companies can present a barrier to effective security.

In considering complexity, we have observed that since cloud computing was developed, the majority of security based research has concentrated on providing technical solutions to solve the security problem. While many excellent solutions have been proposed, cloud security can never be achieved by technical means alone. First, the core business architecture comprises a combination of people, process and technology, thus a solution which addresses only one of these key elements will always be doomed to failure.

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

Third, the additional complexities which cloud brings into the security equation must be recognised, and dealt with appropriately. Increased complexity brings with it increased risk. Simply put, complexity means that such relationships are not easily analysed or disentangled. Thus, it is vital that effort is put in to analysing and disentangling these relationships fully in order to properly understand the risk involved. If this risk is not recognised, and dealt with appropriately, this will inhibit the possibility of achieving good security.

Currently, cloud users effectively have to treat cloud services as a black box, since they have no control over what goes on inside, or behind the scenes. This puts cloud users at a singular disadvantage when it comes to issues of privacy and security. Regulators are taking a far more aggressive approach to breaches, and the cloud user is the one who ends up carrying the can and getting the punitive fines issued by the regulator.

This leads to the issue of lack of responsibility and accountability. Standard service level agreement (SLA) offerings from the major players currently ignore accountability, assurance, audit, confidentiality, compliance, integrity, privacy, responsibility and security, merely offering availability as the focus of their measure of performance. The onus for measuring and proving unacceptable performance is neatly passed to the customer, which, with the inclusion of some suitably deeply buried clauses in the small print, assures the buck invariably never stops with the CSP.

Companies who are cloud users are quite properly legally held responsible and accountable to a variety of regulators throughout industry under privacy and security regulations. Fines for non-compliance are reaching punitive levels, and many regulators have extreme levels of sanction at their disposal. Yet, CSPs are not held to account for their often not inconsiderable role in such failures!

This issue with CSP SLAs is not a trivial issue to address. CSPs need to provide users with assurance, through compliance and audit, that they can provide a level of service capable of meeting user requirements in confidentiality, integrity, privacy and security. CSPs should be prepared to offer cloud users performance guarantees in all their required areas, not just on availability. CSPs need to become accountable to users for meeting these requirements, by which means they will be able to demonstrate a responsible and ethical approach to their customers, and at the same time, providing an extremely robust and dependable service to all cloud users.

We further argue that the CSPs should provide monitoring tools to collect sufficient information to demonstrate that they have achieved the required level of performance, rather than leaving it for customers to find out when something goes wrong. CSPs are much better placed to do this, since cloud customers will not necessarily have access to all the systems necessary for this to happen. We have further argued [13] that this will require a significant change in attitude from the CSPs, leading to the development of better security oriented SLAs, which will improve the approach to security for all actors within the cloud ecosystem.

This was the basis on which, with Pym, we developed a conceptual framework for cloud security assurance[1], expanding on earlier works [14][15], which seeks to address the issues faced in trying to achieve security in the cloud, and provides a more effective means for business to achieve both cloud security assurance along with appropriate standards

compliance, by providing continuous assurance through both compliance and audit.

We draw on natural resource management research [6][16] which provides some very clear illustrations of the effectiveness of stewardship, presenting a clear systems view of the issues addressed. The framework we have proposed addresses these key challenges facing cloud users.

III. How our Framework Operates

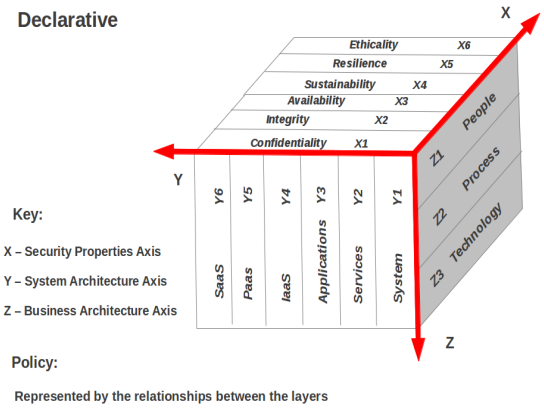

Fig. 1. A Declarative Cloud Three-Dimensional Security Matrix

The framework functions by taking a 3 dimensional security approach to how the company is organised. On one dimension there is the business architecture, which covers people, process and technology; the second dimension covers the security properties, which extends the traditional CIA approach by adding sustainability, resilience and ethics; and the third dimension is the systems architecture of the business, which addresses the systems, services and applications used by the business, to which we must add the cloud models of infrastructure, platform and software as a service (IaaS), (PaaS) and (SaaS). The framework then identifies and addresses every point in the matrix where each of the three dimensions intersect.

There are 4 stages of process involved in running the model. There is the declarative stage, where management set the goals to be achieved. Next the operational stage collects data to measure how well the company is meeting these declarative goals. Then, internal audit will provide assurance through audit and compliance checks to confirm the integrity of the process. Finally, external audit will essentially double check that everything undertaken will have been compliant and thus compliance with standards can be achieved, together with the assurance that the declarative goals of management are being met.

Thus, management need to determine their declarative position on each of these intersecting points, and further, must determine how performance will be measured. Management are responsible for defining proper measurements and metrics to be used in the framework, and this is what we will now address.

IV. Measurement Literature

Measurement mechanisms in accounting and management are well understood and mature disciplines. These measurement mechanisms, while not always trivial, are aided by the common currency of such measures, namely money. Every measure or metric used can be translated into financial terms, which have long been well understood in these fields.

However, the recent development and emphasis of more esoteric management methods, such as corporate social responsibility, sustainability, ethical behaviour and stewardship have brought with them new challenges in respect of how success can be measured. We see a similar problem arising with cloud ecosystems, where issues of security, privacy, sustainability, resilience, ethicality, accountability, auditability and information stewardship also present new challenges in respect of how to measure the success of these values.

Hahn et al [17], suggest the mainstream of the literature on corporate sustainability follows the win-win paradigm, according to which economic, environmental and social sustainability aspects can be achieved simultaneously. The authors argue that trade-offs and conflicts in corporate sustainability are the rule rather than the exception, and propose an initial framework for the analysis of trade-offs in corporate sustainability. They further suggest the question of how such trade-offs can be measured and managed has not been addressed widely.

Lindgreen and Swaen [18] suggest the research community suffers from a lack of understanding of how to develop corporate social performance measures. The authors analyse how companies address these issues, and call for more research in this area. Wood [19] reviews the literature on corporate social performance measurement and sets that literature into a theoretical context. The author emphasises the need for scholars to refocus on stakeholders and society, incorporating literature from other domains in the process.

Green and Peloza [20] seek to understand how consumers define corporate social responsibility (CSR) and how it can enhance the overall value proposition for consumers, but note the inconsistency with which measurement metrics are applied across industry, finding 39 difference metrics in their study. The authors suggest a more explicit and precise measurement of value customers receive in exchange value is needed.

Bodeau et al [21] describe the initial representative set of cyber resiliency metrics identified by the assessment task of the RAMBO project under the FY11 MITRE Innovation Program. The authors suggest that this set of metrics is expected to evolve in response to practical experience as well as to the ongoing refinement of the cyber resiliency engineering framework. Carvalho et al [22], looking at supply chain resilience, propose a conceptual framework for the analysis of relationships between agile and resilient approaches, supply chain competitiveness and performance. The authors propose operational and economic performance measures to facilitate the monitoring of the influence of these practices on supply chain performance.

Looking at corporate sustainability, Christofi et al [23] suggest that the newly created TBL (triple bottom line — economic, environmental and social) reporting practices need to undergo further standardisation and enforcement to avoid,

or give early warnings about, future corporate mismanagement that leads to socio-economic consequences detrimental to investors and consumers in general. The Sustainability Accounting Standards Board [24] has been set up with this purpose in mind.

Eccles et al [25], in looking at how to become a sustainable company, suggest that companies need leadership commitment, an ability to engage with multiple stakeholders along the value chain, widespread employee engagement and disciplined mechanisms for execution. Rahman and Post [26], who are looking at environmental corporate social responsibility (ECSR), develop a transparent ECSR measure, with an explicit coding scheme, that strictly relies on publicly available data. Vieira et al [27] address resilience benchmarking for information systems, and suggest resilience benchmarking merges concepts from performance, dependability, and security. They present an overview on the state-of-the-art on benchmarking performance, dependability and security.

Delmas et al [28] ask what CSR ratings really capture. The authors identify the principal components of corporate environmental performance. They find corporate financial performance to be associated with process but not with outcome measures. Lee et al [29] develop a survey tool which organisations can use to identify their strengths and weaknesses and to develop and evaluate the effectiveness of their resilience strategies and investments.

Linkov et al [30] focus on the development of measurable resilience management systems for use in decision making and government policy. The authors suggest that resilience measurement must be advanced with the use of novel analytic approaches that are complementary to, but readily distinguishable from those already identified with risk management. Linkov et al [31] note that despite the national and international importance of resilience metrics, used to inform management decisions, the measures are still in the early stages of development. The authors develop and organise effective resilience metrics for cyber systems. These metrics link national policy goals to specific system measures, such that resource allocation decisions can be translated into actionable interventions and investments. The authors have identified and assessed a number of metrics using quantitative and qualitative measures found in the literature. They have proposed a generic approach which could integrate actual data, technical judgement, and literature-based measures to assess system resilience across physical, information, cognitive, and social domains.

Prior and Hagmann [32] note that a significant challenge still lies in the accurate characterisation and quantification of resilience, and thus also the ability to provide a systematic basis for policy-making in resilience-based threat mitigation. The authors maintain that resilience should not be reduced to a methodological problem only, given that the methodological operationalisation of resilience also connects with analytical ideas of what and whose kind of responsibility should be measured and political conceptions of who assumes what tasks and responsibility in a resilience framework.

Eccles et al [33] investigate the effect of corporate sustainability on organisational processes and performance, using a sample of 180 US companies. The authors provide evidence that high sustainability companies significantly outperform their counterparts over the long-term, both in terms of stock market as well as accounting performance. Ioannidis et al [34], in addressing resilience in information stewardship, present a mathematical model to measure resilience. Montiel and Delgado-Ceballos [35] carry out a survey of CSR and show that the CSR field is still evolving, with the use of different approaches to define, theorise, and measure CSR. The authors also find differences between the literature that targets scholars versus the one targeting practitioners, and provide a set of recommendations on how to advance the CSR field.

V. How to Develop Useful Measurements

Defining a generic set of measures is unlikely to be useful, since every business is different. This is a task for management. However, we think it will be useful to provide some general assistance by way of a few examples of how to go about it. We will start by looking at each dimension in turn.

The business architecture breaks down into three main areas, people, process and technology. Measuring people can be relatively straightforward. Each employee has a unique employee number, a unique computer access code and password, and access rights to whatever areas are appropriate for carrying out their job. Some companies will already have electronic or biometric systems installed and functioning, others might not, but identifying who is who ought to be relatively straightforward. Most companies will have their processes well documented with a unique reference number assigned to each process.

While these processes may well have been documented for a considerable period of time, it is important to recognise that they may have been defined before security formed part of the requirements. This should be recognised and appropriate steps taken to address this. Technology, too, should be simple enough, as each piece of technology, whether servers, desktop, or mobile device will have a unique asset number, and internet connectivity can be recorded via the unique media access control (MAC) address inside the hardware, as well as the internet protocol (IP) address used to connect to the network, whether from inside the company, or from outside the company via the internet.

Looking at systems next, each piece of technology will have one or more operating systems, which will be identifiable. There will be one or more services running on the equipment, which will be identifiable, and there will be one or more applications running on the equipment, all of which will be identifiable. Where access to cloud systems is available, this will be either at a high level, such as SaaS or some service such as desktop as a service (DaaS), which can be identified. Equally, if the access is to a lower level of service such as PaaS or IaaS, this too can be identified. There may be multiple systems accessed, operated by multiple providers, which may also involve brokers or other service providers, all of which can be identified.

This brings us to a more difficult area, the security properties. Confidentiality can be achieved by ensuring only the correctly authorised people can be granted access to confidential information. This can be achieved by proper access control, and monitoring. Integrity is slightly more challenging, as it is technically more challenging to ensure that information, once

saved into a system has not been tampered with, particularly in the case of databases.

However, this can be addressed by logging every change made to every transaction within a system, logging who made the change, when, from what location and so on. Thus each change in the information state can be preserved, which would allow recreation of the original if the change was malicious.

However, our requirement to address the new security properties of sustainability, resilience and ethics presents the biggest challenge. We could address sustainability of security by using redundancy to ensure continuity of operations in the event of some business disaster or major security breach. This may involve an element of lost time due to set up and configuration time needed to restore systems.

Resilience could be addressed by having a permanently running system mirror which allows for an extremely rapid recovery from unexpected shock. The additional costs of addressing sustainability and resilience would need to be considered. For business critical systems, the additional costs of ensuring sustainability and resilience may end up providing cheap insurance.

Ethics, which generally would include company approach to corporate social responsibility, could be addressed by viewing how suppliers approach these issues, usually disclosed in annual reports, corporate social responsibility reports or on the company website.

Clearly CSPs who concentrate on availability in their SLAs without considering accountability, assurance, audit, confidentiality, compliance, integrity, privacy, responsibility and security, thus leaving the cloud user to carry the can, might well be considered as irresponsible and unethical in their behaviour. The same might be said for companies who provide poor service in other areas, such as outsourced activities which might have an impact on security and privacy.

VI. Addressing a Critical Remaining Obstacle to Cloud Security

We would like to think that there are no weaknesses in the conceptual framework we have developed for cloud security assurance. But to do so would be naïve, as the framework has been necessarily developed to address all aspects of cloud security under the control of the company operating the framework. Unfortunately, the very mechanism of cloud computing means that not all areas are completely under the control of the company operating the framework. At least one or more companies involved in the cloud ecosystem will not be under the control of the company operating the framework, and this presents a key weakness.

There has been a great deal of research carried out into cloud security, and much of this research proposes excellent technical solutions. However, information security in the cloud cannot be solved by technical solutions alone. Business operates through a combination of people, process and technology, thus it is essential to approach security addressing all three of these areas together. This also explains why much of the research carried out in the field of cloud security will be ineffective.

Our proposed framework addresses all three areas of people, process and technology, yet is still not foolproof, and here are some of the main reasons for this: CSP SLA limitations, and unwillingness to change; The threat environment; Standards issues; Management reluctance to take security seriously. One of the most important of these is the SLA between the company and the CSP. It is no accident that the standard SLA offerings from the major CSPs focus on availability. Their business model is geared to providing availability as the main service performance measure to which they purport to be accountable.

Accountability, assurance, audit, confidentiality, compliance, integrity, privacy, responsibility and security do not feature in the standard SLA. It is important that companies recognise that this represents the current status. Any additional requirements must be negotiated directly with the CSP.

Another key area to be considered is the magnitude of the threat environment. Companies are bound by legislation, sometimes regulation, the need to comply with standards, industry best practice and are accountable for their actions. The bad guys have no such constraints. They are completely free to bend every rule in the book, do whatever they want, manipulate, cajole, hack or whatever it takes to get to the money. Also, there are a lot of them out there. Many have different agendas, different skills levels, capabilities and resources at their disposal. Between them all, they can attack 24/7, 365 days a year. They don't work to rule, go home at 5:00pm, take weekends off or go on holiday, at least not until they have relieved you of your cash, and in that case there are plenty more happy to take their place. In addition to which, [36] suggest that over 200,000 new malware threats are being developed globally every day.

Companies who have achieved compliance with a cloud security standard often think they can sit back and relax. They need to think again! There is currently no such thing as a comprehensive cloud security standard, and there possibly never will be. Technology develops so fast, and the standards process, especially for international standards, is so cumbersome that by the time a standard is finally agreed and published, it is likely to be out of date. Sometimes there is a reluctance on the part of management to take security seriously. It is often seen as a technical issue passed to the IT department. Proper security can never be achieved using technical means alone. Business operates with a combination of people, process and technology, not technology alone. Thus it is vital to factor in the impact that all three will have on achieving and maintaining proper security. This needs to be driven from the top. Management need to be fully aware that it is not simply a technical issue, rather it is a fundamental business process which needs to be driven right from the top of the organisation. Information security now presents one of the largest risks facing business today and needs to be given the proper attention and commitment it deserves.

We are concerned about developing proper metrics for the six security goals of our proposed security assurance model. This will not be a trivial exercise and clearly we cannot do justice to all these areas within the space of this paper. Accordingly, we will address each of these areas individually during the next year as part of our ongoing research.

VII. 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 briefly outlined how our cloud security assurance framework operates, and have discussed how the above issues must additionally be addressed.

In looking at measurement literature, we see how some aspects are quite mature and well understood, but that more modern methods of management such as sustainability, resilience and ethics present new challenges due to the dearth of research in these areas. In looking at how our framework operates, we have discussed how the best security approach needs to consider not just a technical solution, but must address people, process and technology.

We have touched on how these difficult areas of security might be approached as part of a comprehensive security solution based on our proposed framework. Clearly, companies could benefit from further research in several of these areas, and in particular, measurement. 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, 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.

[2] 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.

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

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

[5] A. Kolk, "Sustainability, Accountability and Corporate Governance: Exploring Multinationals' Reporting Practices," *Bus. Strateg. Environ.*, vol. 17, no. 1, pp. 1—- 15, 2008.

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

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

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

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

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

[11] F. Pallas, "An Agency Perspective to Cloud Computing," in *Econ. Grids, Clouds, Syst. Serv.* Springer, 2014, pp. 36–51.

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

[13] B. Duncan and M. Whittington, "Enhancing Cloud Security and Privacy: Broadening the Service Level Agreement," in *The 14th IEEE International Conference on Trust, Security and Privacy in Computing and Comms (IEEE TrustCom-15)*. Helsinki, Finland 2015.

[14] A. Beautement and D. Pym, "Structured systems economics for security management," in *WEIS*, 2010, pp. 1–20.

[15] A. Baldwin, Y. Beres, M. C. Mont, S. Shiu, G. Duggan, H. Johnson, and C. Middup, "An Experiment in Decision Making WEIS 2011," in *WEIS*, 2011, pp. 1–28.

[16] R. Kao, *Stewardship Based Economics*. World Scientific, 2007.

[17] 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, pp. 217–229, 2010.

[18] A. Lindgreen and V. Swaen, "Corporate social responsibility," *Int. J. Manag. Rev.*, vol. 12, pp. 1–7, 2010.

[19] D. J. Wood, "Measuring corporate social performance: A review," *Int. J. Manag. Rev.*, vol. 12, pp. 50–84, 2010.

[20] T. Green and J. Peloza, "How does corporate social responsibility create value for consumers?" *J. Consum. Mark.*, vol. 28, pp. 48–56, 2011.

[21] D. Bodeau, R. Graubart, L. Lapadula, A. Rosenthal, and J. Brennan, "Cyber Resiliency Metrics ,," *MITRE Rep. MP 120053 Rev 1.*, no. April, pp. 1–40, 2012.

[22] 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, pp. 49–62, 2012.

[23] 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.

[24] SASB, "Sustainability Accounting Standards Board," http://www.sasb.org/, 2015

[25] R. Eccles, K. Perkins, and G. Serafeim, "How to become a sustainable company," *MIT Sloan Manag. Rev.*, vol. 53, pp. 43–50, 2012.

[26] 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, pp. 307–319, 2012.

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

[28] 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.

[29] 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.

[30] 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 actionable policy," *Environ. Sci. Technol.*, vol. 47, no. ii, pp. 10 108–10 110, 2013.

[31] 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, pp. 471–476, 2013.

[32] T. Prior and J. Hagmann, "Measuring resilience: methodological and political challenges of a trend security concept," *J. Risk Res.*, no. January 2015, pp. 37–41, 2013.

[33] R. 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.

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

[35] I. Montiel and J. Delgado-Ceballos, "Defining and Measuring Corporate Sustainability: Are We There Yet?" *Organ. Environ.*, pp. 1–27, 2014.

[36] Kaspersky, "Global Corporate IT Security Risks: 2013," Tech. Rep. May, 2013.