Company Management Approaches — Stewardship or Agency: Which Promotes Better Security in Cloud Ecosystems?

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*—Historically, companies have been managed under the principles of agency theory. There is evidence to suggest that the complexity of modern computing systems, and in particular cloud computing systems, has become so convoluted that the principles of agency theory can no longer cope. We suggest that the adoption of stewardship theory for cloud security can present a possible credible alternative that can deliver much better results for the security of all cloud users, particularly in the long run.**

Keywords–Stewardship; agency; management; security; cloud computing.

I. Introduction

Modern information systems have evolved considerably over the past four decades, leading to the development of complex, highly distributed information systems and the need to police them properly. The need to address traditional security issues of confidentiality, integrity and availability (CIA) has increased this complexity further, due to the need for scalability and redundancy. As a consequence, despite the benefits offered by Moore's Law [1], costs have increased significantly. The statutory and regulatory environment is also ever increasing in reporting requirements, responsibilities and complexity, leading to an ever increasing additional cost burden. Fines for non-compliance are increasing year on year as regulators take a more and more aggressive approach. One regulator in the UK, the Financial Conduct Authority (FCA) [2] has so far levied fines of £1,427,943,800 during 2014. Contrast this with the level of fines levied by their predecessor, the Financial Standards Authority (FSA) [3], five years ago of £34,800,000.

Cloud computing offers the possibility of a substantial economic benefit to firms, yet at the same time, increases complexity and risk further. This results in an interesting dilemma. On the one hand, potential cost savings of 50 - 90% [4] are possible, which is highly attractive, but on the other hand, complexity can increase exponentially, placing significant increasing risk on business and government alike.

The practice of achieving compliance with recognised security standards is spreading. While this is a good idea in principle, in practice it may not provide the assurance being sought. The multiplicity of security standards currently available, and in particular, the lack of consensus on cloud security standards presents a difficult challenge. Compliance does not necessarily ensure protection. The procedures in use for achieving accreditation often vary enormously, with no real requirement for a rigorous approach. Checklists are often favoured over a deep and searching approach to security standards compliance [5], and there is generally no requirement for regular review.

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

The remainder of the paper is organized as follows: in Section II, we discuss three main barriers to effective cloud security; in Section III, we consider the merits of agency versus stewardship; in Section IV, we demonstrate how each impact on cloud security; and in Section V, we discuss our conclusions.

II. The Challenges

We discuss three main challenges to be overcome when considering information security in the cloud - standards compliance, the limitations on management of agency theory and the sheer complexity of cloud ecosystems.

A. Standards

The recent development and rapid evolution of cloud ecosystems presents a far more rich and complex security environment than existing security mechanisms were designed to cope with. There is a danger that continued reliance on existing standards will lead to real weaknesses in systems which can be vulnerable to exploitation. The challenge here is to develop a means of identifying potential exposure in as comprehensive a manner as possible, yet be sufficiently flexible to adapt with a dynamically changing information ecosystem environment. There are a number of cloud security standards which have recently evolved, but the problem is, which standard should be used? Should it be the Association for Retail Technology Standards (ARTS) [6], the Cloud Security Alliance (CSA) [7], the Cloud Standards Organisation (CSCC) [8], the Distributed Management Task Force (DMTF) [9], the European Union Agency for Network and Information Security (ENISA) [10], the European Telecomminications Standards Institute (ETSI) [11], the Federal Risk and Authorization Management Program (FedRamp) [12], Generally Accepted Privacy Principles (GAPP) [13], the Global Inter-Cloud Technology Forum (GICTF) [14], the International Organization for Standardization (ISO) [15], the ITU Telecommunication Standardization Sector (ITU) [16], the National Insitute of Standards and Technology (NIST) [17], the Organization for the Advancement of Structured Information Standards (OASIS) [18], the Open Cloud Consortium (OCC) [19], the Open Grid

Forum (OGF) [20], the Object Management Group (OMG) [21], the Payment Card Industry (PCI) [22] or the Storage Networking Industry Association (SNIA) [23], to name but a few? None of these standards provides a comprehensive level of complete security — there is no "one size covers all", which also presents a limitation. Even compliance with every single standard will not guarantee complete security, which, in turn, presents yet another disadvantage [24]. While the universal implementation of such standards is often perceived as a laudable aim, there is a fundamental flaw where new computing technology is concerned, namely that the pace of evolution of new technology far outstrips the capability of international standards organisations to keep up with the changes [25]. In addition to which, latest estimates [26] suggest that over 200,000 new malware threats are being developed globally every day. We addressed this in earlier work [24][27].

B. Agency

Another issue arises where the principals of companies utilise the principles of corporate governance [28][29], based on agency theory. Jensen and Meckling [30] recognized that while both principal and agent were utility maximizers, they would not necessarily always have the same alignment of goals. Further, the agent is more likely to have complete knowledge, whereas the principal's generally is incomplete, and this can disadvantage the principal, or at least require the expenditure of additional sums to try to safeguard the position of the principal. Over time, agents, having complete information, can make more decisions which do not fully benefit the princpals, resulting in better utility for themselves. It is very rare that the goals of principal and agent will perfectly align, thus gaining mutual satisfaction, and this is the fundamental flaw agency theory highlights. The business environment is constantly changing, as are corporate governance rules, with more emphasis now being placed on responsibility and accountability [31], social conscience [32], sustainability [33][34], resilience [35] and ethics [36]. We focus on this challenge in the current paper.

C. Complexity

Yet another issue is the increasing complexity which new technology brings, and the ever increasing potential exposure to risk brought about by a failure to grasp the significance of risks arising as a result of this increase in complexity [37]. Traditional distributed information systems present a multiplicity of technical layers, each of which must interact with one or nore other layers. Rather than simplifying this process, cloud introduces yet more layers. There is Infrastructure, Platform and Software as a Service (IaaS, Paas and SaaS), each of which can be operated by different actors. Cloud brokers may also be involved, leading to yet more layers, yet more complexity, yet more risk. Thus, there is a need for a more agile, effective, approach to address these issues. Another hurdle to be overcome is the cross disciplinary nature of today's corporate world. There is more cross-over between disciplines than in the past, which means no single discipline can effectively deal with all the issues arising from the use of cloud technology [38]. Existing security paradigms have not kept pace with the rapidity of development, change and complexity in modern information ecosystems. There is a danger that continued reliance on existing models will lead to real weaknesses in systems which can be vulnerable to exploitation. The challenge here is to develop a means of addressing these weaknesses at a conceptual level which can be demonstrably more robust than the existing mechanisms currently in place. We address this challenge in our future work.

III. Agency vs Stewardship

In order to compare the relative merits of agency against stewardship, it is necessary to understand more clearly what each is and how they work. In the following sub sections, we outline a definition of each and their limitations, followed by a comparison.

A. The Agency Theory of Management

Management has been a focus of academic study for a great many years. Initially, companies were managed by their owners, which is still the model today for many fledgling small businesses. Over time, companies grew larger and larger, resulting in their becoming too large for an individual to be able to provide them with sufficient capital to meet their needs and cover their potential liabilities. The root of this problem can be traced back to the modern corporation, as discussed by Berle and Means [39], creating a separation between ownership and control of wealth. While owners would generally prefer to manage and control their own companies to maximize their own utility for themselves, the large scale of the "modern corporation" puts information management, massive capital needs and economic obligations far beyond the reach of the individual. This increase in size, and capital requirements, led to companies being managed by professional managers (agents) on behalf of the company owners (principals) which led to the development of agency theory.

B. The Definition of Agency Theory

Jensen and Meckling [30] provide us with a definition of agency theory: *"We define an agency relationship as a contract under which one or more persons (the principal(s)) engage another person (the agent) to perform some service on their behalf which involves delegating some decision making authority to the agent. If both parties to the relationship are utility maximizers, there is good reason to believe that the agent will not always act in the best interests of the principal. The principal can limit divergences from his interest by establishing appropriate incentives for the agent and by incurring monitoring costs designed to limit the aberrant activities of the agent. In addition in some situations it will pay the agent to expend resources (bonding costs) to guarantee that he will not take certain actions which would harm the principal or to ensure that the principal will be compensated if he does take such actions".*

Some examples of this relationship are:

- The electorate (principal) and government (agent);
- Shareholders (principal) and Chief Executive Officer (agent);
- Employers (principal) and employees (agent);
- Contractee (principal) and contractor (agent).

There is not a single relationship within a company. Rather the relationship cascades through the organisation and into the outside world. Thus, for example, shareholder to CEO, CEO to business managers, business managers to staff, company to suppliers, customers to company, cloud user to cloud service provider and every sub contracted relationship.

C. The Limitations of Agency Theory

Jensen and Meckling recognised that while both principal and agent were utility maximisers, they would not necessarily always have the same alignment of goals. Further, the agent is more likely to have complete knowledge, whereas the principal generally has incomplete knowledge, and this can disadvantage the principal, or at least require the expenditure of additional sums to try to safeguard the position of the principal. Over time, agents, having complete information, can make more and more decisions which do not fully benefit the princpals, resulting in better utility for themselves. It is very rare that the goals of principal and agent will perfectly align, resulting in mutual satisfaction, and this is both the fundamental insight and flaw in relying upon agency for successful delegation.

D. The Stewardship Theory of Management

The implications of agency theory, agents adhering to the terms of their contract without necessarily achieving the principal's desired outcomes, are problematic and the literature has considered the more principle-based stewardship approach. This has been discussed over several decades, across a number of disciplines, such as accounting [40][41], management research [42][43][44], information stewardship [45][46], where Pym et al specifically focus on cloud stewardship, and in natural resource management [35], where Chapin et al demonstrate, using a systems view, the benefits of the stewardship approach, as does Kao [47].

E. The Definition of Stewardship Theory

Davis [43] provides a good definition of stewardship theory:

"In stewardship theory, the model of man is based on a steward whose behavior is ordered such that pro-organizational, collectivistic behaviors have higher utility than individualistic self-serving behaviors. Given a choice between self-serving behavior and pro-organizational behavior, a steward's behavior will not depart from the interests of his or her organization. A steward will not substitue or trade self-serving behaviors for cooperative behaviors. Thus, even where the interests of the steward and the principal are not aligned, the steward places higher value on cooperation than defection (terms found in game theory). Because the steward perceives greater utility in cooperative behavior and behaves accordingly, his or her behavior can be considered rational.

According to stewardship theory, the behavior of a steward is collective, because the steward seeks to attain the objectives of the organization (e.g., sales growth or profitability). This behavior in turn will benefit principals such as outside owners (through positive effects on profits on dividends and share prices) and also pricipals who are managerial superordinates, because their objectives are furthered by the steward. Stewardship theorists assume a strong relationship between the success of the organization and the principal's satisfaction. A steward protects and maximises shareholders' wealth through firm performance, because, by so doing, the steward's utility functions are maximised".

F. The Limitations of Stewardship Theory

The limitations found in agency theory do not apply in stewardship theory. Since the utility of the steward is firmly in alignment with the utility of the principals, this removes the temptation to make decisions solely for the benefit of the steward. Any decision that benefits the principals will also benefit the steward, and conversely any decision that benefits the steward will also benefit the principals. The only proviso here is the need to provide a sufficient means to incentivise the business manager to become a steward, rather than a self-serving agent.

G. Stewardship Synergy with Cloud Ecosystems

There is a natural synergy between stewardship and cloud ecosystems [48]. Cloud ecosystems are dependent on the building and maintaining of robust relationships between all the actors in the ecosystems [49]. This dependency arises out of a need for sustainability, resilience and ethicality. In order for a greater take up of cloud usage, there needs to be trust and a mutual accountability between all the actors involved. The multiplicity of actor relationships and this need for responsibility and accountability means that the traditional agency approach cannot succeed. The cloud ecosystem is too rich an environment for the agency approach to be able to succeed, whereas stewardship is tailor made to handle this level of complexity [50].

The EU recognizes the existence of this complexity in relationships, especially with regard to information security in the cloud, and has produced a working paper [51] for discussion on the subject. The ISO 27000 standards, while they address the notion of security, are not yet sufficiently well developed to fully cover these issues. There is no doubt they will be expanded to cover these issues in time. They do recognise the existence of corporate outsourcing, but as yet this has not been fully adapted to cover all the modern extensions of this mechanism, including offshoring and cloud.

We believe a stewardship approach represents an ideal mechanism to address the shortcomings which presently exist. This approach may provide a useful means to help businesses to adopt cloud more readily, to better reap the benefits and economies offered, while maintaining a better grasp of the security implications associated with such a move.

H. Why the Time is Right for Change

The culmination of years of self-serving behaviour on the part of managers has led to more extreme agent behaviour [52]. Also, it leads to a short term view of running a business, and this can work against the long term sustainability of the business and impact adversely on resilience. It can also lead to driving managers into behaving less ethically due to these pressures to perform in the short term. Equally, the agency behaviour of large scale shareholders has helped to encourage this behaviour in managers, as these shareholders are frequently looking for the best short term returns. Thus, the effects of greed by both managers and certain shareholders seem to take agency theory to a logical extreme. There is no mechanism in agency theory to deal with the broad themes of sustainability, resilience and ethicality. It is no coincidence that this behaviour is particularly prevalent in the banking industry.

During the past 15 years, Enron and other scandals led to the passing of the Sarbanes-Oxley Act [53] in the United States of America (USA). In 2008, the banking crisis arrived, with all the attendant fall out. There have been countless corporate frauds of some magnitude, such as the Madoff scandal. There is a perception among shareholders that the prescriptions to

deal with agency theory no longer work to reign in the worst excesses of corporate management [52].

Indeed, in the five years prior to the financial crisis of 2008, the annual report of the Royal Bank of Scotland (RBS) made much of their stewardship of the business. In the 2007 annual report [54] published in spring 2008, the then Sir Fred Goodwin used stewardship language in his Group Chief Executive's review, stating "Our results demonstrate the resilience of the Group in the face of testing circumstances." These claims of stewardship were clearly a sham, as that resilience rather catastrophically ran out on 7 October 2008.

Corporate managers themselves are beginning to see the effect their "fat cat" bonuses and incentive schemes are having on shareholders, to the point that many are now voluntarily agreeing to reduce or even give up their entitlement, especially where the business does not perform so well. Shareholders are looking for a return to "the good old days", when corporate managers were looked on as honourable people, who put the interests of the business first, and their own interests second. In essence, they embodied many of the core values of stewardship.

I. Agency vs Stewardship Summary

In Table I, we can see the major differences between agency and stewardship, the psychological and situational mechanisms involved.

Since the utility of the steward is in alignment with the utility of the principal, this removes the temptation to make decisions solely for the benefit of the steward. Any decision that benefits the principal will also benefit the steward. The stakeholders and relationships in a business are not, of course, limited to managers and shareholders. Customers, suppliers, government, audit firms and even the local communities are stakeholders in the business. As noted above, in corporate governance today, we see much more consideration being given to the the notion of corporate social responsibility, resilience, sustainability and an ethical approach to doing business. There is certainly more pressure on managers in today's business world to take a more outward view of their actions, potentially leading to a more responsible stewardship approach. There is an ever growing appetite for more accountability in business, being driven both by shareholders, government, customers, suppliers, auditors and the general public.

TABLE I. A COMPARISON OF AGENCY AND STEWARDSHIP[43]

	Agency Theory	**Stewardship Theory**
Model of man	Economic man	Self-actualizing man
Behaviour	Self-serving	Collective serving
Psychological Mechanism		
Motivation	Lower order/economic needs (psychological, security, economic)	Higher order needs (growth, achievement, self-actualization)
Social Comparison	Extrinsic Other managers	Intrinsic Principal
Identification	Low value committment	High value committment
Power	Institutional (legitimate, coercive, reward)	Personal (expert, referent)
Situational Mechanism		
Management Philosophy	Control oriented	
Risk orientation	Control oriented	Involvement oriented
Time frame	Short term	Long term
Objective	Cost control	Performance enhancement
Cultural Differences	Individualism High power distance	Collectivism Low power distance

It is clear that the culmination of years of self-serving behaviour on the part of business managers has led to agency behaviour moving beyond its own limitations. It would seem the fundamental flaw with agency theory is that it cannot cope with unbridled greed. Also, it leads to a short term view of running a business, and this can work against the long term sustainability of the business and impact adversely on resilience. It can also lead to driving managers into behaving less ethically due to these pressures to perform in the short term. Equally, the agency behaviour of large scale shareholders has helped to encourage this behaviour in managers as the shareholders are frequently looking for the best short term returns.

Thus, the effects of greed on both the part of managers and shareholders push agency theory beyond its capabilities. There is no mechanism in agency theory to deal with sustainability, resilience and ethicality. At the time agency theory was developed, such concerns were of little relevance, but in today's business world, that is no longer the case.

In Table II, we can see how the major differences between adopting agency and stewardship affect the relationship between the manager and the shareholders.

TABLE II. A PRINCIPAL-MANAGER CHOICE MODEL[43]

Principal's Choice

Manager's Choice	*Agent*	*Steward*
Agent	Minimize Potential Costs Mutual Agency Relationship 1	Agent Acts Opportunistically Principal is Angry Principal is Betrayed 2
Steward	3 Principal Acts Opportunistically Manager is Frustrated Manager is Betrayed	4 Maximize Potential Performance Mutual Stewardship Relationship

Where manager and shareholder both adopt the agency approach, there can be mutual satisfaction as long as their respective goals are in alignment, but, as has already happened in many cases, over time this can lead to a mutually destructive relationship developing.

Where manager and shareholder adopt an opposite approach, with one adopting an agency approach and the other adopting a stewardship approach, there will be a disparity between the outcomes for each, regardless of which adopts which position.

Where both manager and shareholder alike are prepared to adopt a stewardship approach, their joint goals are much better aligned, and the extreme pressures and destructive nature of the short-term approach can be set aside. This mutually beneficial approach also serves to handle the additional requirements of sustainability, resilience and ethicality for the business, which will benefit both parties. This allows for a long-term view to be developed by all concerned, which will result in a far better outcome for everyone.

IV. Impact on Cloud Security

So, the question is how does management approach impact on cloud security?

Cloud service providers (CSP) have developed their cloud business models using agency theory. The standard SLA offerings from the major players basically ignore accountability, assurance, audit, compliance, integrity, privacy and security. Instead, they merely offer availability as the focus of their measure of performance. The onus for measuring and proving unacceptable performance is neatly passed to the customer, which, with the inclusion of some suitably deeply buried clauses in the small print, assures the buck invariably never stops with the CSP.

Of course it is possible to negotiate an SLA to include these missing measures, but you can be sure the cost of good corporate lawyers and the increased service costs involved will decimate any potential cost savings offered by the cloud paradigm. Since such costs would, in any event, only be affordable by the largest corporations, this puts most small and medium-sized enterprises (SME) and sole traders at a commercial disadvantage.

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

Compliance with security standards can be viewed as an agency reaction by company management to protect them from being sued by their own principals for failing to implement proper security. Since current standards are neither complete, nor up to date, compliance with these standards cannot ensure security [24].

In Table III, we can see how the Cloud User - CSP Choice Model can lead to an improvement in this situation. CSPs can no longer afford to "stick their heads in the cloud" when it comes to information security. There is no "I" in team. Every actor in the cloud ecosystem needs to contribute towards better security for society as a whole. Growth in global security breaches increased by more than twice the rate of global gross domestic product (GDP) increase during 2014 [55]. Failure to tackle this issue means this situation will only get worse.

TABLE III. Cloud User-CSP Choice Model[43]

		Cloud User(Principal)'s Choice	
		Cloud User(Agent)	*Cloud User(Steward)*
CSP's Choice	*CSP(Agent)*	Minimize Potential Costs Mutual Agency Relationship Security is fair 1	CSP Acts Opportunistically Cloud User is Angry Cloud User is Betrayed Security is poor 2
	CSP(Steward)	3 Cloud User Acts Opportunistically CSP is Frustrated CSP is Betrayed Security is poor	4 Maximize Potential Performance Mutual Stewardship Relationship Security is good

Every actor in the cloud ecosystem is responsible for maintaining good security. That means in addition to top management, middle and lower management must equally be committed, as must all the company's employees. Company suppliers and company customers too must play their part. A major component of the cloud ecosystem is of course the service providers who provide every element of the system, whether they are providing PaaS, IaaS, SaaS or some other aspect "as a service". All actors must be prepared to be accountable for ensuring a proper level of security is maintained and every relationship has the potential to be managed as an agency or stewardship one. Service providers must be prepared to ensure SLAs can be re-written to more fairly spread risk and accountability between all the actors to ensure better security of the whole. Company auditors must also recognise the risk involved in the use of cloud systems and must be more vigilant to ensure areas of weakness are highlighted and dealt with properly in good time. The threat environment is not going to improve for the better any time soon.

V. Conclusion

Thus, we can see that every member of the cloud ecosystem needs to be more aware of their role within the system. Each has their part to play. There are a great many potential weaknesses in cloud ecosystems. While these can be identified and addressed to ensure proper levels of security can be achieved and maintained, there is no doubt that as long as the agency approach persists, with all the actors pursuing their own agendas, it will be extremely difficult to achieve a satisfactory level of security.

It is certainly the case that the extremes of agency behaviour can lead to lower levels of security being achieved within cloud ecosystems. Conversely, a stewardship approach can lead to a more robust security stance, which can provide additional resilience and sustainability in the long run for a company. Given the rapidly evolving nature of the threat environment, it is no longer a question of if a company will be compromised, but rather it is a question of when, and for how much? With the added possibility of punitive regulatory fines and the adverse impact on reputation and share price, companies would do well to take serious notice of this issue.

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 would also argue that following decades of corporate excess brought about by the worst of agency behaviour, it would be appropriate for corporate management to consider taking a step change in their outlook towards a stewardship based management style. This would not only promote long term sustainability and resilience of companies, but would lead to a more honest approach to information security. We would further argue that this will require a significant change in attitude from the cloud service providers, leading to the development of better security oriented SLAs, which will improve the approach to security for all actors within the cloud ecosystem.

The next step is to consider how a stewardship approach, requiring a high level of trust, can be encouraged as seeming practical rather than naïve; this will inevitably require increased transparency and the welcoming of high quality monitoring by all sides.

REFERENCES

[1] G. E. Moore, "Cramming More Components onto Integrated Circuits," Electronics, no. April 19, 1965, pp. 114-117.

[2] FCA, "Fines Table - 2014," 2014. [URL]: http://www.fca.org.uk/firms/being-regulated/enforcement/fines retrieved: Jan 2015

[3] P. Taylor, "FSA fines double to record 35m in 2009," 2009. [URL]: http://www.telegraph.co.uk/finance/newsbysector/banksandfinance/6852385/FSA-fines-double-to-record-35m-in-2009.html retrieved: Jan 2015

[4] P. Mell and T. Grance, "Effectively and Securely Using the Cloud Computing Paradigm," Tech. Rep., 2009.

[5] B. Duncan and M. Whittington, "Reflecting on Whether Checklists Can Tick the Box for Cloud Security." in Cloud Comp. Tech. Sci. (CloudCom), 2014 IEEE 6th Int. Conf. Singapore: IEEE, 2014, pp. 1-6.

[6] ARTS, "Association for Retail Technology Standards," 2014. [URL]: https://nrf.com/resources/retail-technology-standards-0 retrieved: Jan 2015

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

[8] CSO, "Cloud Standards," 2013. [URL]: http://cloud-standards.org/ retrieved: Jan 2015

[9] DMTF, "Distributed Management Task Force: Standards and Technology," 2014. [URL]: http://www.dmtf.org/standards retrieved: Jan 2015

[10] ENISA, "A Security Analysis of Next Generation Web Standards," 2013. [URL]: http://www.enisa.europa.eu/ retrieved: Jan 2015

[11] ETSI, "European Telecommunications Standards Institute," 2014. [URL]: http://www.etsi.org/standards retrieved: Jan 2015

[12] FedRamp, "FedRamp," 2014. [URL]: http://cloud.cio.gov/fedramp retrieved: Jan 2015

[13] CPA/CA, "Generally Accepted Privacy Principles," Tech. Rep., 2009.

[14] GICTF, "Global Inter-Cloud Technology Forum," 2012. [URL]: http://www.gictf.jp/index_e.html retrieved: Jan 2015

[15] ISO.org, "ISO/IEC 27000:2009 - Information technology - Security techniques - Information security management systems - Overview and vocabulary," ISO.org, Geneva, Switzerland, Tech. Rep., 2009.

[16] ITU, "ITU Telecommunication Standardization Sector," 2014. [URL]: http://www.itu.int/en/ITU-T/publications/Pages/default.aspx retrieved: Jan 2015

[17] NIST, "NIST Security and Privacy Controls for Federal Information Systems and Organizations," Natioinal Institute of Standards and Technology, Gaithersburg, MD, Tech. Rep. February, 2012.

[18] OASIS, "Organization for the Advancement of Structured Information Standards," 2014. [URL]: https://www.oasis-open.org/standards retrieved: Jan 2015

[19] OCC, "Open Cloud Consortium," 2014. [URL]: http://opencloudconsortium.org/working-groups/ retrieved: Jan 2015

[20] OGF, "Open Grid Forum," Tech. Rep.

[21] OMG-CC, "Object Management Group," 2014. [URL]: http://www.cloud-council.org/ retrieved: Jan 2015

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

[23] SNIA, "Cloud Data Management Interface," Tech. Rep., 2010.

[24] 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.

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

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

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

[28] S. Ross, "The Economic Theory of Agency: The Principal's Problem," Am. Econ. Rev., vol. 63, no. 2, 1973, pp. 134-139.

[29] M. Eisenhardt, "Agency Theory : An Assessment and Review," Acad. Manag. Rev., vol. 14, no. 1, 1989, pp. 57-74.

[30] M. C. Jensen and W. H. Meckling, "Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure," J. financ. econ., vol. 3, no. 4, 1976, pp. 305-360.

[31] M. Huse, "Accountability and Creating Accountability: a Framework for Exploring Behavioural Perspectives of Corporate Governance," Br. J. Manag., vol. 16, no. s1, Mar. 2005, pp. S65-S79.

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

[33] 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.

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

[35] 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.

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

[37] E. Zio, "Reliability engineering: Old problems and new challenges," Reliab. Eng. Syst. Saf., vol. 94, no. 2, Feb. 2009, pp. 125-141.

[38] M. Dlamini, J. Eloff, and M. Eloff, "Information security: The moving target," Comput. Secur., vol. 28, no. 3-4, May 2009, pp. 189-198.

[39] A. A. Berle and G. C. Means, The Modern Corporation and Private Property, 1932.

[40] F. y. Gjesdal, "Accounting for Stewardship," J. Account. Res., vol. 19, no. 1, 1981, pp. 208-231.

[41] V. O'Connell, "Reflections on Stewardship Reporting," Account. Horizons, vol. 21, no. 2, Jun. 2007, pp. 215-227.

[42] L. Donaldson, "Stewardship Theory or Agency Theory: CEO Governance and Shareholder Returns," Aust. J. Manag., vol. 16, no. June 1991, 1991, pp. 49-65.

[43] J. H. Davis, F. D. Schoorman, and L. Donaldson, "Toward a Stewardship Theory of Management," Acd. Mgt. Rev., vol. 22, no. 1, 1997, pp. 20-47.

[44] C. E. Crutchley and R. S. Hansen, "A Test of the Agency Theory of Managerial Ownership, Corporate Leverage, and Corporate Dividends," Financ. Manag., vol. 18, no. 4, Jan. 1989, pp. 36-46.

[45] P. S. Licker, "Application Stewardship: A User Responsibility Approach to Post-Implementation Application Performance," MIS Q., 2010, pp. 151-157.

[46] D. Pym, M. Sadler, S. Shiu, and M. C. Mont, "Information Stewardship in the Cloud : A Model-Based Approach," Proc. CloudComp, 2011, pp. 1-20.

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

[48] A. Baldwin, D. Pym, M. Sadler, and S. Shiu, "Information Stewardship in Cloud Ecosystems: Towards Models, Economics, and Delivery," 2011 IEEE Third Int. Conf. Cloud Comput. Technol. Sci., Nov. 2011, pp. 784–791.

[49] D. Pym, M. Sadler, S. Shiu, and M. C. Mont, "Information Stewardship in Cloud Computing," Int. J. Serv. Sci. Manag. Eng. Technol., vol. 1, no. 1, 2010, pp. 50-67.

[50] C. Ioannidis, D. Pym, and J. Williams, "Fixed Costs , Investment Rigidities , and Risk Aversion in Information Security : A Utility-theoretic Approach," 2013, pp. 1-16.

[51] EU, "Unleashing the Potential of Cloud Computing in Europe," 2012. [URL]: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SWD:2012:0271:FIN:EN:PDF retrieved: Jan 2015

[52] J. Harris, "Whats Wrong with Executive Compensation? Jared," J. Bus. Ethics, vol. 85, no. 1, 2009, pp. 1-22.

[53] SOX, "Sarbanes-Oxley Act of 2002," p. 66, 2002. [URL]: news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf retrieved: Jan 2015

[54] RBS, "Royal Bank of Scotland Group Annual Report Year Ending 2007," Royal Bank of Scotland, London, Tech. Rep., 2007.

[55] PwC, "The Global State of Information Security," PwC, Tech. Rep., Jan. 2015. [URL]: http://www.pwc.com/gx/en/consulting-services/information-security-survey/download.jhtml retrieved: Jan 2015