Developing a Conceptual Framework for Cloud Security Assurance

Bob Duncan
Computing Science
University of Aberdeen
Email: bobduncan@abdn.ac.uk

David J. Pym
Computing Science
University of Aberdeen
Email: d.j.pym@abdn.ac.uk

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

***Abstract*—Managing information security in the cloud is a challenge. Traditional checklist approaches to standards compliance may well provide compliance, but do not guarantee to provide security assurance. The complexity of cloud relationships must be acknowledged and explicitly managed by recognising the implications of self-interest of each party involved. We begin development of a conceptual modelling framework for cloud security assurance that can be used as a starting point for effective continuous security assurance, together with a high level of compliance.**

I. Introduction

An important aspect of developing an assurance model for security in the cloud is that it be compliant with best practice in the development and maintenance of information security management systems, (e.g., [1]–[3]). Companies are now subject to a raft of legislative and regulatory requirements and compliance with standards can provide a useful way of ensuring these requirements are met. The corporate business environment is constantly evolving with greater emphasis being placed on responsibility and accountability [4], especially for the security and privacy of data [5].

A number of security standards have recently evolved, but the very number raises the issue of 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 ([2], [6]–[9]), to name but a few? For example, the international ISO 27000 information security management system standard [3] is itself broken down into a considerable number of individual standards. There are currently 21 published standards, 14 at draft stage (around 2 years from being published) and over 7 in study period (around 4 years from being published). The pace of evolution of new technology far outstrips the capability of international standards organizations to keep up with the changes [10].

The business environment is also constantly changing, as are corporate governance rules, with more emphasis now being placed on responsibility and accountability [11], social conscience [12], sustainability ([13], [14]), resilience [15] and ethics [16]. These changes are pushing the traditional principles of corporate governance ([17], [18]) based on agency theory to their limits. Increasing technology complexity heightens exposure to risk, particularly if the potential concomitant problems are not understood or addressed [19]. Thus, there is a need for a more agile and effective approach to address these issues. With 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 [20].

In this paper, we propose a conceptual framework for cloud security assurance, expanding on earlier works ([21], [22]), which seeks to address these issues and provide a more effective means for business to achieve both cloud security assurance along with appropriate standards compliance. We draw on natural resource management research ([15], [23]) which provides some very clear illustrations of the effectiveness of stewardship, presenting a clear systems view of the issues addressed. The remainder of the paper is organized as follows: in Section II we explain the fundamental concepts of information security, exploring the issues faced in more detail, and how these can form a barrier to successful implementation of cloud security assurance; in Section III we look at possible approaches to address these issues; in Section IV we explain our conceptual framework; in Section V we discuss our conclusions.

II. The Issues to be Addressed

The fundamental concepts of information security are confidentiality, integrity, and availability (CIA). Beautement and Pym [21] provide an account of the misunderstandings prevalent in information security which arise through confusion between (declarative) objectives of ([24], [25]) information security operations with the (operational) mechanisms deployed in order to achieve these objectives. For example, to achieve a declarative objective of confidentiality, access control provides the operational mechanism to achieve this. To achieve a declarative objective of availability, hardware redundancy can be deployed as an operational mechanism to achieve this objective. Conceptually, it is important to separate the treatment of each in order to understand how objectives might be delivered. Bearing this in mind, we will concentrate on the three issues outlined in the introduction: the standards issue, the agency issue, and the complexity issue.

A. The Standards Issue

There is a growing trend for large corporates in the UK to move towards ISO 27000 compliance. In 2012, PwC [26] note that almost two thirds of the UK's largest companies are either fully or partially ISO 27000 compliant, thus we shall concentrate on these standards in this paper. As already

stated, the pace of evolution of new technology far outstrips the capability of international standards organizations to keep up with the changes [10], as is particularly evident with the International Standards Organization (ISO). The ISO 27000 [3] series of standards on Information security management systems are not yet fully developed, with over 21 still yet to be published.

Standards such as 27017 cloud computing, 27018 personally identifiable information, 27033 parts 4-6 network security, 27034 part 2-6 application security, 27036 supplier relationships, 27038 digital redaction, 27039 intrusion detection systems, 27040 storage security, 27041-3 digital evidence and 27044 security information and event management, are drafts, implying possibly two years from becoming a published standard. Areas such as electronic discovery, co-ordination of investigative projects, personal information management, taxonomy, ICT supply chain security, 27009 cloud security technology and 27011-19 sector specific implementation, are still in a study period, meaning possibly four years before publication. The principal limitation of these standards is that, by the ISO's own admission, they represent a statement of what to do in order to be compliant, not how to do it. That is left to the individual organization or business. Further, there is a tendency for those engaged in audit compliance work to adhere to checklists, rather than executing due diligence with regard to information security and risk management [27]. Finally, the multiplicity of cloud standards under development throughout the world, with little co-ordination between them, adds to the difficulty.

B. The Agency Issue

The principles of corporate governance ([17], [18]) based on agency theory struggle to adequately handle the rising complexity of organizational relationships and sustainability caused by the increasing reliance on cloud systems. The root of this problem can be traced back to the modern corporation, as discussed by Berle and Means [28], 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, the large scale of the modern corporation puts their massive capital needs and economic obligations far beyond the reach of the individual.

Jensen and Meckling [29] recognized that while both principal (shareholders) and agent (managers) 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. This can disadvantage the principal, or at least require the expenditure of additional sums to try to safeguard their position. Over time agents, having more complete information, can make more decisions which do not fully benefit the principals, resulting in better utility for themselves. It is very rare that the goals of principal and agent will perfectly align, thus maximising mutual satisfaction, and this is the fundamental flaw which agency theory highlights.

C. The Complexity Issue

Cloud computing opens up exposure to new issues. While cloud economics are highly attractive, providing a great driver to use cloud, there are significant issues of security and privacy to consider. There is also an increase in the complexity of systems, the potential number of actors and exposure to new risks [30]. Due to the global structure of many cloud service providers, there are also issues of the sovereignty of data. Where previously everything was stored and operated from within the domain of the organization, with cloud computing this can be enormously more complex and can therefore expose the business to additional unexpected risk. Whether an organization uses the cloud alone for all their business needs, or integrates cloud use into their own, possibly extensively distributed, IT systems - it is clear that ensuring proper security of information is likely to be a non-trivial exercise.

At the most basic level, a simple two-dimensional security matrix can be used. Additional layers of classification or clearance can easily be accommodated. Here, data classification is listed along the top, and the clearance required to access that data is listed along the side. For example, someone with low clearance can access all unclassified data, but are not able to access classified data. However, in a typical large organization utilising an IT system comprising distributed resources and services running over various locations this becomes more complex. Particularly where standards compliance is required, such a system would require mapping onto a three dimensional matrix, such as demonstrated in Figure 1 in order to achieve a declarative view for compliance purposes. This is necessary to reflect the increase in potential relationships between the business architecture, the systems architecture and the security requirements.

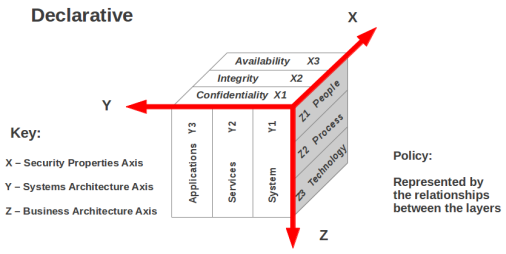

Fig. 1. A Declarative Three-dimensional Security Matrix

This figure can outline the basic declarative position needed for compliance. It demonstrates three interconnected layers: first, there is the security properties layer, which comprises the traditional CIA security properties; next, there is the systems architecture layer, which comprises the system, the services and the applications used; finally, there is the business architecture layer, which comprises people, process and technology (the hardware used for the IT systems). This three-dimensional matrix helps demonstrate the relationships between each of the layers — there are twenty seven potential relationships to consider. These relationships characterize the business policy required to ensure compliance. Thus, the intersection of X1, Y1 and Z1 represents how confidentiality, system and people should be addressed. However, the lack of relevance of the standards, many of which were defined before cloud computing was developed, presents a problem. Indeed, the very mechanisms which make cloud computing economically attractive are at the same time increasing the difficulty and complexity of security issues, which may have a knock on impact on the cost benefits. Yet, finding a means of assessing the impact of cloud

computing on standards compliance should prove attractive for those businesses wishing to benefit from implementing cloud computing.

III. Possible Solutions to these Issues

A. Standards

We must first understand that ISO standards do not yet exist at any sufficient level of detail to enable proper security in cloud computing. Second, any business which has achieved standards compliance on information security management systems, must be under no illusion that they have a secure system. The approach used to achieve compliance under the standards as they currently exist can lead to a false sense of security, which in turn can lead to potential disaster. This can result in putting the business, shareholders, managers, customers, suppliers, government and audit firms at heightened risk of exposure to knock on attacks or other losses or liabilities following unexpected compromise of systems. Third, we can recognize that to achieve the comfort of a good level of security, we need to appreciate the true level of the complexities involved and deal with them appropriately.

B. Agency

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 ([31], [32]), management research ([33]–[35]), information stewardship ([36], [37]), where Pym et al specifically focus on cloud stewardship, and in natural resource management [15], where Chapin et al demonstrate, using a systems view, the benefits of the stewardship approach, as does Kao [23].

Since the utility of the steward (managers) is in alignment with the utility of the principal (shareholders), 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 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. This is accompanied by an ever growing appetite for more accountability in business, being driven both by shareholders, government, customers, suppliers, auditors and the general public.

C. Complexity

A distributed system is by its very nature highly complex, and we must recognize that this is inevitable. Indeed, using cloud increases the complexity further, and we must recognize that, too. We have seen from Figure 1 how we can prepare a simple declarative model of the relationships to be considered in order to ensure the security of a business. We then need to expand this model to allow us to address the importance of today's corporate governance culture, by adding sustainability, resilience and ethicality to the traditional CIA security requirements. We then add IaaS, PaaS and SaaS to cover using the cloud, where each of these services may be provided by different service providers, although this can be reduced where these are serviced by a single supplier. We show in Figure 2 how this expanded model would look.

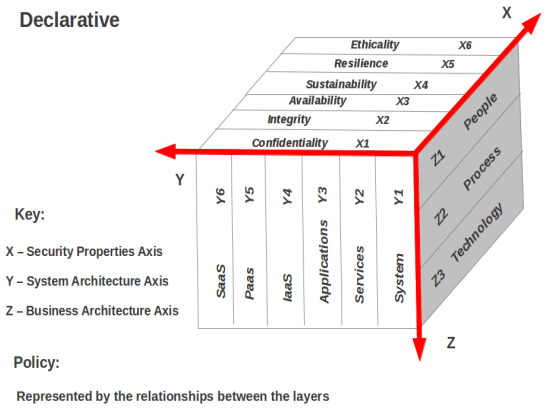

Fig. 2. A Declarative Cloud Three-Dimensional Security Matrix

This increases the number of potential relationships from our original twenty seven, to one hundred and eight, depending upon the number of extra layers needed, but serves well to illustrate the size of the problem. Consideration will also have to be given to the detailed technical composition of the architecture deployed, as it may be necessary to consider far more than the 108 relationships shown here. Providing policy is extended to accommodate these additional relationships, we can see that the declarative position can clearly reflect the additional complexities generated by incorporating cloud use.

D. 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 [39]. It also 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. This can be highlighted by some well-known examples. Enron and other scandals led to the passing of the Sarbanes-Oxley Act [38] in the US. In 2008, the banking crisis occurred, 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 [39].

There is a natural synergy between stewardship and cloud ecosystems [22]. Cloud ecosystems are dependent on the building and maintaining of robust relationships between all the actors in the ecosystems [40]. 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 function efficiently, whereas stewardship can easily handle this level of complexity [41]. The European Commission recognizes the existence of this complexity in relationships, especially with regard to information security in the cloud, and has produced a working paper [44] 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. We believe a stewardship approach, defining relationships by principles rather than rules, represents an ideal mechanism to address the shortcomings which presently exist. This approach may provide a useful means to help businesses 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.

IV. The Conceptual Framework for Cloud Security Assurance

As discussed in Section II there is a clear need to separate declarative and operational layers. We believe it is necessary to add two further layers in order to ensure the effectiveness of the model in operation and to meet corporate governance requirements. We propose to add an assurance layer, which will monitor how effectively the operational layer meets the goals set in the declarative layer; and an audit layer to confirm the whole system is functioning properly and achieving the stated goals.

The process will be iterative in nature. The results achieved by the operational, assurance and audit layers continually provide feedback to the declarative layer which will be used to improve the efficiency of the operation of all layers. We envisage security will involve every employee in the business, customers and supply chain. All have a part to play in the success of ensuring the security of the business. It will be necessary to adapt the model to suit the sector-specific requirements of each business, whether physical, operational, regulatory or otherwise. We can thus divide the assurance model into four main layers: the declarative layer; the operational layer; the assurance layer; and the audit layer. The example high-level declarative model we illustrate in Figure 3 provides an overview of how the layers fit together.

A. The Declarative Layer

It is necessary for management to define very clearly what their security and stewardship position is in respect of each of the intersecting points described in the three-dimensional matrix (see Figure 2), although some will be dictated by statutory or regulatory obligations. We borrow from economic utility theory, for example [43], to introduce a simple economic utility model into these relationships to provide a weighting to reflect the security preferences or requirements of the business, allowing us to develop a simple means of tailoring the model to fit each individual business.

In representing the policy of the organization, there are three main aims for each of the relationships defined in the declarative model: to provide a mechanism for measurement, to define a target position, and to incorporate a utility preference over the target. By way of an example, if we look at co-ordinate $(X3, Y3, Z2)$, this represents "availability for applications to run processes". For each such component of the declarative model, as specified in Figure 2, that is of interest — let's assume we index these components by a variable i — we associate a component U_i of a utility function, as follows:

- Measure: M_i; for example, % uptime of systems hardware; in this case, expressed as an average over time;
- Target: m_i, the declarative target for this operation;
- A function f_i expressing how utility depends on deviation from target. For example, a Linex function [42], usually expressed in the form $g(z) = (exp(\alpha z) - \alpha z - 1)/\alpha^2$, is used to capture a degree of asymmetry that is parametrized by α;
- The weight w_i (between 0 and 1, and $\sum_i w_i = 1$) expressing the managers' weighting/preference for the ith security component of interest;
- This can be expressed thus: $U_i = w_i f_i(M_i - m_i)$;
- System equation $M_i = s_i(x_i)$, where x_i is a vector of control variables and s_i describes M_i's dependency upon them.

Thus the overall utility function is

$$U = \sum_i U_i = \sum_i w_i f_i(M_i - m_i).$$

By introducing suitable stochastic processes into the system functions s_i, we can obtain a treatment of the expected utility of the system. In general, such a treatment of a system's properties will be too complex to have analytic solutions for the control variables, so that simulations must be used. By evaluating each co-ordinate in the declarative layer, the business can define their position on the security risks they face and the resulting utility model of the whole will reflect the level of utility they seek, while ensuring compliance with any standards. It will also be possible to place constraints on the targets. For example, in the above example, the target may be 99.99%, but the constraint may be that availability should never fall below 98%. In analysing all the co-ordinates of this model, it may be that some threats are subsidiary to others, and that by securing the main threat, this eliminates the subsidiary threats, although this may not always be the case. Each business or organization can take a view on whether they cover them individually, or as related groups, as appropriate to suit their particular needs.

B. The Operational Layer

The second layer is the operational layer, which is used to reflect the current status of all existing business processes. In Figure 3, we can now see the relationship between the declarative and the operational layers. The declarative layer provides the goal for the operational layer to reach and provides the tools needed to ensure these goals can be met.

We need to make the assumption that performance data will be available for measurement of the effectiveness of these tools.

By way of an example, in the context of ensuring the confidentiality of personal data of clients, if we look at co-ordinate $(X1, Y2, Z1)$ in Figure 2, this represents "confidentiality of services for people". The following tools and status might then apply: use card access to terminal (to limit physical access to the system); use authentication procedure (to ensure the user is who they claim to be); apply access controls (to ensure the system only allows access to the correct data by users authorized to access that data). However, we need to recognize that performance data will not always be available, in which case it will be necessary to develop suitable heuristics. This data needs to be available to cover each of the relationships in the system, some of which will come from data logging of system events, and it may be useful to use analysis tools to automatically analyse the data and summarize it for ease of interpretation.

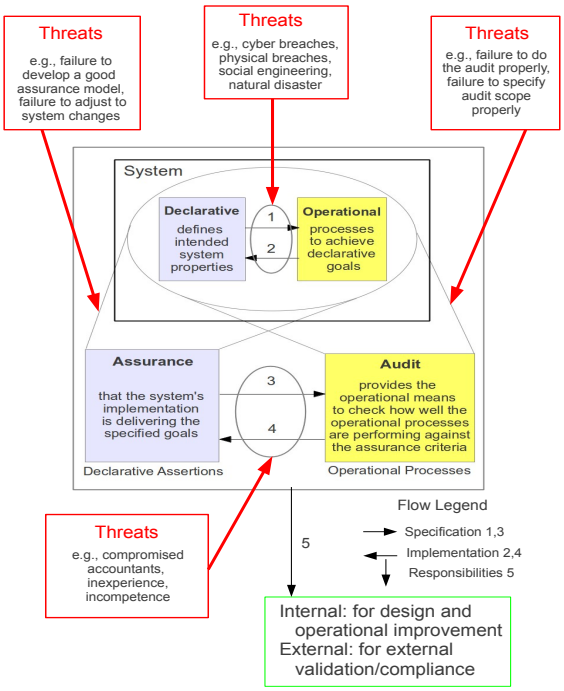

Fig. 3. The Declarative/Operational/Assurance/Audit Layers (see Subsection IV(E) for notes

C. The Assurance Layer

The assurance layer provides the assurance that the system's implementation is delivering the specified goals. It represents a declarative assertion, at a far more detailed level than the declarative layer provides, of what is needed to ensure these goals are met. Figure 3 shows how this layer fits with the declarative and operational layers of the system. Searching questions will need to be asked in order to ascertain how well the assurance layer is helping the operational layer meet these declarative requirements. The idea is to ask difficult questions in order to root out potential weaknesses which might otherwise go unnoticed. This will be an ongoing iterative process, continually searching to uncover weaknesses, and constantly striving to ensure the security goals of confidentiality, integrity, availability, sustainability, resilience and ethicality are met.

D. The Audit Layer

The audit layer provides the operational means to check how well the operational processes are performing. Figure 3 shows how the audit layer fits into the overall relationship between the other layers. The running of the audit layer will be an iterative process, continually searching to uncover weaknesses, and constantly striving to ensure security objectives are maintained.

This function will be carried out at two levels, internally by the internal audit department of the business, and externally by the auditors responsible for certifying compliance with standards. Internal audit will require strong backing from management to ensure it is empowered to perform at the requisite level of effectiveness and this process will be ongoing, providing constant feedback. The external auditors should review the effectiveness of the assurance layer, and should seek to search out weaknesses using long established auditing techniques such as are used in financial reporting. They will need to address each of the relationships of the system to ensure all potential risks are properly identified and properly addressed, not by way of checklists, but rather by exercising due diligence with regard to information security and risk management. This process is likely to be far less frequent than the work carried out by internal audit.

E. How the Layers Interact

Management specify their security and stewardship preferences in the declarative layer, which are passed to the operational layer at (1) in Figure 3. The operational layer provides the necessary tools for implementation, providing the necessary performance data/heuristics. There will be feedback to management at (2). The assurance layer provides the detailed declarative assertions for the system which are fed to the audit layer at (3). The audit layer provides the necessary operational processes to check how effective assurance is, and feeds back to the assurance layer at (4). As we see from (5), the responsibilities for this process are shared internally, by internal audit who will provide input for design/operational improvement, and externally, by the external auditors who will provide the external validation/compliance. These interactions will be highly iterative, responding to the ever changing threats faced by the organization, some of which are shown in Figure 3, with a permanent cycle of information flows back and forth across the layers. The whole process will more effectively inform compliance with whichever standards the business may choose.

V. Conclusion

By extending the use of declarative and operational systems modelling to include an assurance and audit layer for businesses using cloud ecosystems, we can create a suitable framework to improve the effectiveness of cloud security assurance. This framework could provide a more effective continuous monitoring system than is achieved using existing standards compliance mechanisms. The frequency with which

these standards are reviewed is insufficient for proper security assurance. Also, the systems involved are far too rich in complexity to be able to be properly assessed and any meaningful assurance given by means of a checklist.

It is vitally important to differentiate between the declarative and operational layers of an assurance model, but this alone is not enough to be truly effective in assuring an adequate level of security. It is certainly true that defining management security and stewardship policy at the declarative level, and matching these requirements with the operational tools needed to achieve these targets, represents a great improvement on traditional methods of assurance. However, continuous monitoring using the assurance layer tightens the effectiveness of the system substantially. Adding the audit layer — which can now be approached in a more cost effective fashion over time — really serves to produce an assurance model that can actually provide the comfort of an effective level of security. This framework can be mapped onto the requirements of whichever standards are chosen by the business.

A factor common to most of the evolving cloud security standards is the reliance on checklists to establish a "snapshot" view of compliance, on an infrequent temporal basis. This checklist culture can shift the focus away from facing uncomfortable truths in favour of achieving compliance at all costs. The threat environment we live with today continues to evolve, with criminals finding ever more inventive ways to attack. They are relentless in their pursuit, and businesses must become ever more vigilant in order to safeguard their electronic assets. It is time to deploy effective tools in this fight to defend their assets.

REFERENCES

[1] H. M. Gov, "Best Practice Cyber Security and Information Assurance," 2013. [Online]. Available: https://www.gov.uk/government/policy-teams/office-of-cyber-security-and-information-assurance

[2] ENISA, "ENISA Best Practice," 2013. [Online]. Available: http://www.enisa.europa.eu/

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

[4] S. Pearson, "Toward Accountability in the Cloud," *IEEE Int Comp*, 2011.

[5] M. Mowbray & S. Pearson, "A Client-Based Privacy Manager for Cloud Computing," *Proc 4th Int ICST Conf on COMSWARE '09*, 2009.

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

[7] Cloud Security Alliance, "Cloud Standards," 2013. [Online]. Available: https://cloudsecurityalliance.org/

[8] FedRamp, "FedRamp Cloud Security Standards," 2013. [Online]. Available: http://www.fedramp.gov/

[9] PCI, "PCI Security Standards," 2013. [Online]. Available: https://www.pcisecuritystandards.org/

[10] G. T. Willingmyre, "Standards at the Crossroads," *StndView*, 1997.

[11] M. Huse, "Accountability and Creating Accountability: a Framework for Exploring Behavioural Perspectives of Corporate Governance," *Brit J. Mgt*, 2005.

[12] A. Gill, "Corporate Governance as Social Responsibility : A Research Agenda," *Berkeley J. Int'l L.*, 26, 2, 2008.

[13] C. Ioannidis, D. Pym & J. Williams, "Sustainability in information stewardship: Time Preferences, Externalities and Social Co-Ordination," in *WEIS 2013*, 2013, to be published.

[14] A. Kolk, "Sustainability, Accountability and Corporate Governance: Exploring Multinationals' Reporting Practices," *Business Strategy and the Environment*, 17, 1, 2008.

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

[16] S. Arjoon, "Corporate Governance: An Ethical Perspective," *J. Bus Ethics*, 61, 4, 2005.

[17] S. Ross, "The Economic Theory of Agency: The Principal's Problem," *The Amer Econ Rev*, 63, 2, 1973.

[18] M. Eisenhardt, "Agency Theory : An Assessment and Review," *Acad Mgt Rev*, 14, 1, 1989.

[19] E. Zio, "Reliability engineering: Old problems and new challenges," *Reliab Eng & Sys Safety*, 94, 2, 2009.

[20] M. Dlamini, J. Eloff & M. Eloff, "Information security: The moving target," *Comp & Sec*, 28, 3-4, 2009.

[21] A. Beautement & D. Pym, "Structured systems economics for security management," in *WEIS*, 2010.

[22] A. Baldwin, D. Pym, M. Sadler & S. Shiu, "Information Stewardship in Cloud Ecosystems: Towards Models, Economics, and Delivery," *2011 IEEE Third Int Conf Cloud Comp Tech and Sci*, 2011.

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

[24] D. B. Parker, *Fighting Computer Crime: A New Framework for Protecting Information*, S. Bosworth, Ed. Wiley, 1998.

[25] P. G. Neumann, "Comp-Related Risks. 1995," *Addison-Wesley*, 1995.

[26] PwC on behalf of BIS and Infosecurity Europe, "UK Information security breaches survey 2012," 2012. [Online]. Available: http://www.pwc.co.uk/en_UK/uk/assets/pdf/olpapp/uk-information-security-breaches-survey-technical-report.pdf/

[27] House of Lords Select Committee on Economic Affairs, "Big 4 Audit Firms Enquiry," 2013. [Online]. Available: http://www.parliament.uk/business/committees/committees-a-z/lords-select/economic-affairs-committee/news/big-4-auditors-inquiry-report/

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

[29] M. C. Jensen & W. H. Meckling, "Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure," *J. of Fin Econ*, 1976.

[30] W. Jansen & T. Grance, "Guidelines on Security and Privacy in Public Cloud Computing," NIST, Tech. Rep., 2011.

[31] F. Gjesdal, "Accounting for Stewardship," *J. Acc Res*, 19, 1, 1981.

[32] V. O'Connell, "Reflections on Stewardship Reporting," *Acc Hor*, 2007.

[33] L. Donaldson, "Stewardship Theory or Agency Theory: CEO Governance and Shareholder Returns," *Aus J. Mgt*, 16, 1991.

[34] J. H. Davis, F. D. Schoorman & L. Donaldson, "Toward a Stewardship Theory of Management," *Academy of Management Review*, 22, 1, 1997.

[35] C. E. Crutchley & R. S. Hansen, "A Test of the Agency Theory of Managerial Ownership, Corporate Leverage, and Corporate Dividends," *Fin Mgt*, 18, 4, 1989.

[36] P. S. Licker, "Application Stewardship: A User Responsibility Approach to Post-Implementation Application Performance," *MIS Quarterly*, 2010.

[37] D. Pym, M. Sadler, S. Shiu & M. C. Mont, "Information Stewardship in the Cloud : A Model-based Approach," *Proc of the CloudComp*, 2011.

[38] SOX, "Sarbanes-Oxley Act of 2002," p. 66, 2002.

[39] J. Harris, "Whats Wrong with Executive Compensation?," *J. Bus Eth*, 85, 1, 2009.

[40] D. Pym, M. Sadler, S. Shiu & M. C. Mont, "Information Stewardship in Cloud Computing," *Int J. Serv Sci, Mgt, Eng, and Tech*, 1, 1, 2010.

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

[42] A. Zellner, "Bayesian estimation and prediction using asymmetric loss functions," 1986.

[43] R. Keeney & H. Raiffa, *Decisions with Multiple Objectives: Preferences and Value Trade-Offs*. Wiley/Cambridge University Press, 1993.

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