Compliance with standards, assurance and audit: does this equal security?

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

Mark Whittington
Accountancy and Finance
University of Aberdeen
mark.whittington@abdn.ac.uk

ABSTRACT
Managing information security is a challenge. Traditional checklist approaches to meeting standards may well provide compliance, but do not guarantee to provide security assurance. The same might be said for audit. The complexity of IT relationships must be acknowledged and explicitly managed by recognising the implications of the self-interest of each party involved. We show how tensions between these parties can lead to a misalignment of the goals of security and what needs to be done to ensure this does not happen.

Categories and Subject Descriptors
H.4 [**Information Systems Applications**]: Miscellaneous; D.2.8 [**Software Engineering**]: Metrics—*complexity measures, performance measures*

General Terms
Theory

Keywords
Standards, assurance, audit, security, compliance, checklists

1. INTRODUCTION
When people discuss IT security, the words compliance, assurance, and audit are frequently referred to. However, the four words security, compliance, assurance and audit are not interchangeable and may even be perceived differently by those from different backgrounds or professions. It would be logical for a company to aim for complete security as long as it could be attained at a reasonable cost. The Oxford English Dictionary [40] has two useful definitions of security — "The safety of an organization, establishment, or building from espionage, criminal activity, illegal entrance or escape, etc." and "With reference to cyber-security: the state of being protected against the criminal or unauthorized use of electronic data, or the measures to achieve this." It is, however, difficult for a company to know if it is secure, especially as this is likely to be a moving target over time and be affected by changes in internal processes or the outside environment. The company's management can seek to assure itself of security through assurance (OED: "A promise or engagement making a thing certain; a formal engagement, pledge, or guarantee; a positive declaration intended to give confidence") through employing individual or corporate experts to interrogate the company's processes and internal activities.

It is even more difficult for an outsider, a customer or supplier for example, to be confident that a company is secure; the outsider is looking for objective evidence of security, or at least that there is an awareness of security issues and of taking it seriously. This evidence can take two forms: compliance or audit. Compliance (OED: "The action or fact of complying with a wish or command") requires a code or set of standards against which the company's activities and processes can be compared and either match (compliant) or fall short (non-compliant). The evidence of security that a compliance check list provides depends on a number of factors including the knowledge and independence of those who wrote the code and whether it is still pertinent to today's environment. Audit (OED: "To make an official systematic examination of (accounts), so as to ascertain their accuracy") requires outsiders who are deemed to be both objective and expert to form their own opinion of what is being audited and then to publically state their confidence (or otherwise) in the reliability of what they have investigated. Auditing is not straightforward or easy. Just as with accounting auditors, objectivity is difficult when companies pay auditors themselves and auditors would like to be retained for the following year. Audit is also potentially very expensive if done well by the best experts in the field and there is a temptation to reduce the experts' role to one of advising, often writing checklists to be administered by qualified technicians. Boritz and Timoshenko [14] discuss the use of checklists and it is clear that a great deal of care and adaptation is necessary if they are to be more effective than individual judgement and the checklist becomes more of a thought-starter than a series of boxes to tick.

The potential economic benefits offered by the adoption of cloud technology are well documented, but these benefits can be marred by the introduction of additional problems, such as security, privacy, legal, sovereignty issues, and the difficulty of auditing transactions due to the complexities of the technology. These challenges are not insurmountable, but there is no doubt that they present an increase in the

risks faced by companies who wish to take this route, as well as an increase in the costs of attaining a given level of security. These challenges also promote a tension between the actors involved, for example between regulators, corporate managers and auditors. We can see from Figure 1 how these tensions can lead to a misalignment of the goals of security. Each of the four dimensions overlaps, however, none guarantee full security.

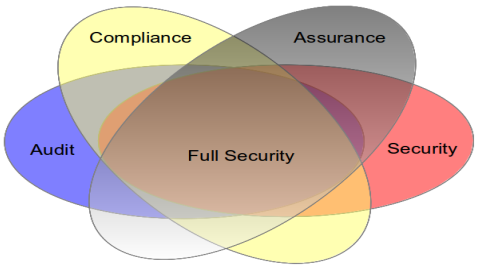

Figure 1: The Effect of the Tension Between Actors

The remainder of the paper is organized as follows: in Section 2 we discuss standards, their history and the reason for them and why they are important; in Section 3 we consider what compliance means and how it might be achieved; in Section 4 we look at assurance; in Section 5 we look at audit and in Section 6 we consider what security means; in Section 7 we consider whether there is a way forward and in Section 8 we discuss our conclusions.

2. STANDARDS

Setting standards has been a human preoccupation for many centuries and is not new or unique to computer science. We give three brief examples to set the standard setting scene. Why do we have standards, what are they and what do we use them for? Standards have been around for a very long time. One of the earliest examples of standardization is the creation of a calendar, an invaluable boon for helping farm crops. Over 20,000 years ago, our Ice Age ancestors in Europe made the first rudimentary attempts to keep track of days by scratching lines in caves and gouging holes in sticks and bones. In 1120 AD, King Henry I of England standardized measurement by instituting the ell, which was equivalent to the length of his arm, in order to provide a degree of uniformity for trade.

Standards to assess the good behaviour of companies also evolved over time and through lessons from bad experiences. In the UK, the South Sea Company, was established in 1711 to trade in the Spanish South American colonies, but met with poor success, culminating in the "South Sea Bubble" disaster of 1720. This and other financial disasters would ultimately lead to the creation of the Joint Stock Companies Act 1844, under which it was possible through a simple registration procedure to incorporate, hence regulating a standard for corporate organisation. Further Companies Acts defined more controls to ensure growing governance of companies. These standards of corporate governance tend to be expressed in very general terms, albeit penalties for failure to comply may be involved, including prison terms in some cases.

However, as companies became more and more complex, government chose to regulate certain industries, for example, banking, finance, insurance, telecommunications, transport, aerospace, arms manufacture, oil, gas, pharmaceuticals, energy generation and distribution, medical, professional services, agriculture and food production. With regulation, a regulator is appointed to oversee standards of behaviour within a whole industry. The regulator will usually have power of sanction, generally extending to large fines and possible suspension of ability to trade within the industry. Such broad and focussed regulation still did not lead to the standards of behaviour that the standards setters envisaged. Following financial de-regulation in the 1980s which led to extremes of corporate financial excess, government responded to this by commissioning the 1992 Cadbury Report [16], which resulted in the publication of the Combined Code of Corporate Governance. This code of practice applies to all large public companies, and attempts to set standards of good corporate governance — adopting a more relaxed approach of "comply or explain". The Code is regularly updated to reflect the changing business environment.

We can see that whether we talk about legislation, regulation or standards, the common thread running through is that they are reactive in nature. They respond to a particular need which means they are always likely to be behind what is happening now. There will always be a lead time between deciding something is needed and achieving implementation, which may take several years. This becomes more of an issue for international standards due to the differing agendas being pursued by different countries, which can further increase the time lag to implementation. The problem is yet further exacerbated in a technological environment, such as security in computing, and especially in a fast moving technology like cloud computing. However, not only is technology rapidly changing, but the threat environment is also developing at a considerable pace [18].

The fundamental concepts of information security are confidentiality, integrity, and availability (CIA). Beautement and Pym [11] provide an account of the misunderstandings prevalent in information security which arise through confusion between (declarative) objectives of ([41, 38]) information security management systems 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. Conceptually, it is important to separate the treatment of each in order to understand how objectives might be delivered.

Cloud computing presents us with an excellent example of how standards are set, trail and even compete with each other within a computer science environment. A number of security standards have recently evolved, but the very number raises the additional 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 ([25, 27, 24, 43, 23]). For example, the international ISO 27000 information security management system standard [33] is itself then broken down

into a considerable number of individual standards. There are currently 21 published standards within this ISO set, 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 these changes [53]. This plethora of new cloud security standards which are evolving can create some degree of confusion as to which should be adopted. Yet there is no one-size-fits-all approach that can be used to address all the security needs of companies. Security standards evolved long before the evolution of cloud computing, and the NIST SP800-53 [39] standard is one such example.

The NIST standard was developed by NIST to further its statutory responsibilities under the Federal Information Security Management Act (FISMA) 2002. The standard forms the basis for regulation and is designed to improve the security of federal information systems. NIST incorporates controls from ISO 27002 with other government and non-government frameworks.

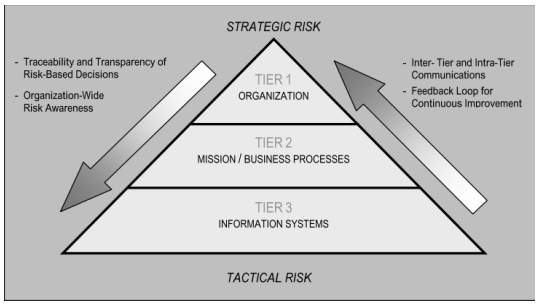

Figure 2: The NIST 3 Tiered Risk Management Approach [39]

As we can see from Figure 2, the NIST standard takes a three tier risk management approach to information security. This demonstrates the top down nature of the approach, which aims to engender reliability, trustworthiness and resilience in the business. Of course, these particular standards were developed before cloud computing evolved, although NIST subsequently addressed this area. The Cloud Security Alliance (CSA), a not for profit organisation with a mission to "promote the use of best practices for providing security assurance within Cloud Computing and to provide education on the uses of Cloud Computing to help secure all other forms of computing", really attacked this area. As we can see in Figure 3, the CSA have created a three dimensional model to reflect the complexities of the differing cloud service models. However, it should also be borne in mind that NIST is primarily aimed at government agencies. The problem here is that publicly traded organizations are not bound by the same security assumptions and requirements as government agencies. Indeed more stringent cost considerations might also be a limiting factor.

The changing demands of security are evidenced by the following statement accompanying the release of CSA v3.0: [24] *"The CSA guidance as it enters its third edition seeks to establish a stable, secure baseline for cloud operations. This effort provides a practical, actionable road map to managers wanting to adopt the cloud paradigm safely and securely. Domains have been rewritten to emphasize security, stability and privacy, ensuring corporate privacy in a multi-tenant environment. In the third edition, the guidance assumes a structural maturity in parallel with multinational cloud standards development in both structure and content. Version 3 extends the content included in previous versions with practical recommendations and requirements that can be measured and audited".*

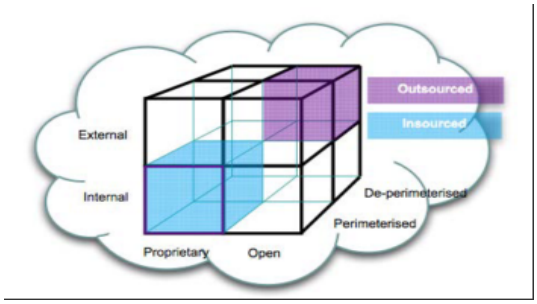

Figure 3: The CSA Cloud Cube [24]

There is a growing trend for global corporates to move towards ISO 27000 compliance. In 2012, PwC [45] note that almost two thirds of the UK's largest companies are either fully or partially ISO 27000 compliant. The ISO 27001 approach uses the Plan, Do, Check, Act model (PDCA), as we can see in Figure 4

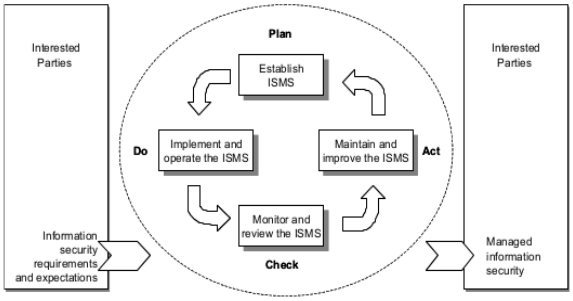

Figure 4: The ISO Plan, Do, Check, Act Model [33]

Most of the ISO 27000 cloud standards are either still at draft or in a study period. 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 company. 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 [1]. Also, in a great many cases, implementation of these security standards is often delegated to the IT department of the company. Information Security Governance is a business decision. Boards of Directors and Senior Management must be involved to effectively lead the cultural change needed, commit capital and human resources, make appropriate changes to HR metrics, policy and job descriptions.

In looking at just these three standards, NIST, CSA and ISO27000, we can see there is much common ground between them. Yet there are differences too, and this presents another of the problems of adopting standards, namely the lack of complementarity between them, meaning no one standard covers all needs.

3. COMPLIANCE

Along with the development of standards came the need to seek compliance. In a business context, legislation is enacted for a specific purpose, for example the tax laws are designed to collect the correct amount of taxation due by every company. Each company must prepare annual accounts, which form the basis from which tax computations are made to calculate the correct amount of taxes due to be paid. The complexities of the various Taxes Acts are such that teams of accountants and sometimes lawyers are invariably involved in this process, as non-compliance can result in punitive fines or even criminal charges being brought against the company, directors, or both.

Where a business operates within a regulated industry, the regulator for the industry sets the standards which must be complied with. Sometimes these standards evolve through consultation with the industry. Compliance is generally regulated by means of recommendations for change, fines (sometimes particularly large) or in a worst case, by revocation of a license to operate within the industry.

All large public companies operating within the UK are subject to the Combined Code of Corporate Governance. The Code is designed to ensure high ethical standards, attention to corporate social responsibility and proper assessment of risk are maintained in the top UK companies. All directors must now be subject to a regular skills audit to ensure that they have a sufficient level of competence to carry out their duties within the company. Reporting is carried out through the Annual Report, in which the board must "Comply or Explain" their position on all elements of the Code. There are no formal sanctions for non-compliance, rather any non-compliant director will find considerable difficulty in acquiring future directorships. Large non-compliant companies are likely to find their directors appearing before parliamentary committees, with all the adverse publicity which that entails. Witness the fall out from the banking crisis in recent years and the removal of key executives from power.

If we return to the international security standard ISO 27000, some two thirds of UK companies listed in the FTSE100 index are either fully or partially compliant. Compliance is achieved after a review and audit of business processes under the terms of the detailed standards the company has chosen to comply with. Providing the company can meet the required standard, they will achieve compliance. Compliance can be revoked should the company fail to maintain the required standards over time.

Some industries publish "Best Practice" guidelines, with the expectation that those operating within the industry would follow these practices. There is no obligation to do so, but in the event that a company decides not to comply and for some reason becomes involved in litigation, the fact of their non-compliance will be taken into account in any judgement and will undermine their position.

In most of the above compliance cases, there is a common thread running through them all, namely the method of achieving compliance. This all too often relies on a checklist approach, which lacks the application of searching questions used in the traditional auditing approach applied to the annual report. Also, the frequency, or lack of, standards compliance monitoring can also be an issue. Just as with accounting, the audited Annual Report gives a measure of reassurance, but it does not ensure the company will not go bankrupt a few days after the accounts are published.

In 2011, IsecT [32] presented a superficial introduction to information security frameworks, covering security standards, laws, regulations and security recommendations or obligations of various kinds. They attempt to explain why 'everyone is always going on about security compliance'. The frequency of compliance auditing is generally quite relaxed, in that reassessment need take place only when system changes take place, or every few years, otherwise. This fails to address the rapidly evolving nature of security threats, and the clear need to employ some method of continuous monitoring when it comes to security management. Reports from global security companies [45, 50, 52] suggest that over 85% of security breaches involve a low level of technical competence, facilitated instead by lack of understanding, lack of competence, or poor configuration of systems on the part of victims.

4. ASSURANCE

BS5750 [15] was an early quality assurance standard introduced in 1979. Assurance of computer systems followed later, with, for example, the Business and Industry Advisory Committee to the OECD [13] publishing some guidelines for the security of networks and information systems. Security assurance for intelligent complex systems became of increasing interest with Pham et al [42] and with Goertzel et al [28] publishing a state-of-the-art report on behalf of the Information Assurance Technology Analysis Center (IATAC) and the Data and Analysis Center for Software (DACS). The IT Governance Institute (ITGI) published a new executive summary framework [19] for Control Objectives for Information and Related Technology (COBIT) compliance, along with the detailed [30] guidelines. Baldwin et al [10], described an enterprise assurance model allowing many layers of the enterprise architecture, from the business processes, supporting applications and the IT infrastructure and operating processes, to be represented and related from a control and risk perspective. Midgley et al [36] called for the use of more simplified models in complex fields.

The area continued to develop with Beres et al [12], presenting an innovative way to assess the effectiveness of security controls where measurable aspects of controls are first captured in the models and then the models are used to analyse the security data gathered from the IT environment. Collinson and Pym [22], presented some contributions to the process-theoretic and logical foundations of discrete event modelling with resources and processes. The Information Systems Audit and Control Association (ISACA) [31] published guidance which established the direction for the information security program and expectations as to how in-

formation is to be used, shared, transmitted and destroyed. The Open Web Application Security Project (OWASP) also published their Software Assurance Maturity Model (SAMM) [35]. Collinson et al [21], described a mathematical framework to handle semantics for structured systems modelling and simulation.

In 2011, the Open Data Center Alliance [8, 5, 6, 4, 7] published a number of proposals, including a cloud provider security assurance model. Alexander et al [2] suggest there are sufficient similarities between safety systems, for which there is wide use of assurance cases, and security systems to allow the adaption of safety systems assurance cases for use in security systems. We can see that assurance of security in an IT setting is a developing field, implying there is still more progress to be made.

5. AUDIT

Auditing in the accountancy world has enjoyed the benefit of over a century of practice and experience. Despite this, there remain differences of opinion and a number of problems yet to be resolved. One of the main issues concerns the independence of the auditor. The auditor is meant to be independent, yet is paid by the firm they are auditing. There may be additional links between the auditor and the firm, such as other non-audit consulting work undertaken by the auditor. An audit firm is keen to remain auditor of the firm for a long period of time to ensure continuity of income and enhancement of profit. The firm is often keen not to change auditor too frequently, lest their reputation suffer damage by being unable to retain an auditor, as well as attempting to keep costs to a reasonable level. Audit firms are keen to undertake non-audit consultancy work in order to further maximise revenue and profits. The firm is generally keen for this practice to take place, due to perceived cost savings to the firm. These arrangements can potentially create tensions between the two, which in some circumstances might affect the impartiality of the auditor.

The accounting profession has been considering the feasibility and economics of continuous assurance [3], while recognising the importance of corporate governance in ensuring sound financial reporting and deterring fraud. Cohen et al [20] examined the impact of various corporate governance factors, such as the board of directors and the audit committee, on the audit process and conducted a semi-structured interview with 36 auditors on current audit practices in considering corporate governance in the audit process. They found that auditors view management as the primary driver of corporate governance. The inclusion of top management in the "corporate governance mosaic" is inconsistent with agency theory's prescription of the board and other mechanisms serving as a means to independently oversee management's actions to protect stakeholders.

Ramamoorti [46] considered the establishment, growth, and evolution of the contemporary internal auditing profession and Moeller [37] considered how the role of internal auditing has changed since the introduction of the Sarbanes-Oxley Act of 2002 [47]. Zeff [54] examined the historical evolution in the United States of the use of the term "present fairly" in the auditor's report, as well as the experience and arguments in the United States and Canada regarding the use of a "two-part" opinion in the report. He then developed an argument for the adoption of a "two-part" opinion, decoupling "present fairly" from conformity with generally accepted accounting principles, which would place primary emphasis on "present fairly". Archambeault et al [9] consider the need for an internal audit report (IAR) to increase governance transparency for external stakeholders. They conclude that an IAR has potential to complement existing governance disclosures, increase stakeholder confidence in governance quality, and motivate internal audit diligence, while recognising that further research is needed.

In contrast, IT audit is relatively new on the scene, and has therefore some way to go to reach a decent level of maturity. Given that accounting research is much more advanced, and yet it has taken over a century for accounting audit to reach a point where there remains a number of unresolved problems, clearly there will be much more research needed in the field of computing audit. It is of particular concern that IT audit is not regulated to anything like the same extent as accounting audit, and this prompts the question of just how effective it might be.

6. SECURITY

This section aims to highlight that the global IT business risk threat environment is not static. It is constantly evolving as criminals discover new vulnerabilities and novel methods of exploiting them. There are few barriers to entry. No large corporate building needs to be set up, no expensive equipment is needed, no degree qualified staff are required, no extensive staff hierarchy. A simple desktop, laptop or notebook, an internet connection and a few spare pounds to buy a "starter pack" of hacking tools and a "prospect list" and they are in business. They can operate from any country, and they can access any company in any country they choose. Of course, there are those who simply do it for fun, or for the "buzz" of getting into secure systems.

However, at the other end of the scale, there are also state-sponsored organizations, such as those from China [29], who are very knowledgeable, have access to sophisticated equipment, and are heavily bankrolled. There are also activist groups who are generally not out to steal money or trade secrets, but wish to expose perceived "wrongdoing" on the part of large corporates. There is also the internal threat to consider. Disaffected employees, laziness, sloppy installation of systems, simple naivety or perhaps lack of training in the importance of security. Software products, too, can pose a threat. Default user names with easily cracked passwords, or back-doors can present a hidden risk. Failure to check security logs can also present a problem. Some of these risks are virtually impossible to guard against, but many are easy, and cheap, to tackle, yet many companies fall down at this elementary stage.

There are a number of annual reports produced by a variety of specialist security companies who report on the global cyber threat environment. While these have been fairly sparse over the years, since 2010, they have become a regular feature in response to the worsening cyber-security environment. In their 2010 report, Cisco [17] note the shift in cyber-criminals' focus away from PCs towards mobile platforms, and are also noticing a greater exploitation of Apple prod-

ucts. The authors believe that the reason for this is that PC manufacturers are building better security into their products, thus making life much more difficult for cybercriminals.

Kaspersky [34] made particular note of the 8 fold increase in drive-by attacks targeting vulnerabilities in user browsers. The authors also commented on the increased sophistication of attacks. PWC [44] carried out an information security breaches survey who note that social networks and software as a service have moved Internet use beyond websites and email, creating new vulnerabilities. Criminals are also adapting their techniques and cybercrime is becoming more common. After falling for the last few years, the cost of security breaches appears to be rising fast. The most dramatic growth is in external attacks which have trebled since 2008. They note that more complex threats have emerged over the last two years. Technical controls are no longer, in isolation, enough to protect organisations. A combination of people, technology and process is now required. To succeed in today's environment, organisations need to think several moves ahead of the criminals. Staff and customers need to be more aware of security threats. Collaborative working practices offer real opportunities, but create a demand for assurance across the supply chain.

Trend [48] note that cybercriminals are driven by money. The money is primarily found where there is a large monoculture or where applications containing lots of valuable data are found. Today this means PCs and Macs are mainly targeted, but shifts in the technology industry coupled with business and consumer adoption mean that these targets are changing. In the future, mobile devices like smartphones and the public/private cloud will become greater targets for cybercrime. Trend suggest that attacks will become more targeted, they note the increase in drive-by infections, and suggest that new attack vectors will be developed to target virtualized and cloud environments. Trend [49] dubbed 2011 the "Year of Data Breaches," as they witnessed organizations world-wide succumb to targeted breach attacks that soiled their reputations via the loss of confidential information and caused them to spend huge sums of money on fixing the damage done. Two of the biggest targets — RSA and Sony Play Station — were left with no other choice but to publicly disclose facts about the attacks against their infrastructure so their customers could ensure proper mitigation. They note that during 2011, they have seen an exponential increase in mobile attacks where mobile malware invaded device users privacy by stealing personal and other kinds of confidential information. The authors also note the increase in social engineering attacks on social networking sites from both spammers and scammers.

In 2012, PWC [45] in their report on information security breaches, note that security breaches remain at historically high levels, costing UK plc billions of pounds every year. A big driver of this is the continuing escalation of cyber-attacks. The number of significant hacking attacks on large organisations has doubled over the last two years. The authors are also seeing many data protection breaches, data loss events and computer frauds, particularly in organisations that haven't invested in staff education. Most serious breaches result from failings in a combination of people, process and technology and they suggest it is important to invest in all three aspects. Social networks are growing in importance to business, and companies are rapidly opening up their systems to smart phones and tablets. Security controls are lagging behind the rate of technology adoption.

Trend [51] disclose that most notable for 2012 is that it took Android less than three years to reach the volume of malware threats that it took 14 years for the PC to reach. Attackers moved their traditional attacks to social media platforms like Pinterest and Tumblr for a broader reach. Attackers have even embraced social media for command and control, opting for Twitter over IRC in some cases. Cisco [18] note that cybercriminals are taking advantage of the rapidly expanding attack surface found in today's "any-to-any" world, where individuals are using any device to access business applications in a network environment that utilizes decentralized cloud services and highlight global threat trends based on real-world data, and provide insight and analysis that helps businesses and governments improve their security posturing for the future and suggest that today's enterprises may be unprepared for the reality of navigating an "any- to-any" world — at least, from a security perspective. The authors suggest that global data center traffic is expected to quadruple over the next five years, and the fastest-growing component is cloud data. The authors anticipate that by 2016, global cloud traffic will make up nearly two-thirds of total data center traffic. In spite of the complexities of current systems, there is evidence that cybercriminals are sticking to simple tried and tested techniques, relying instead on the slack attitudes towards security of some firms.

7. IS THERE A WAY FORWARD?

The above list of concerns and problems may lead to pessimism. We can see from the previous sections that while there is no shortage of research in each of these areas, there are a number of issues which still need to be addressed. Legislation, regulation, standards, good corporate governance and best practice all share the common shortcoming of lack of currency. Ironically, in the early stages of development, there is also the issue of lack of maturity. Under any new regime, it will take time for regulators and practitioners alike to understand fully the finer points of what they are dealing with. Some industries take an economic view that to achieve 95% compliance will be far more cost effective than achieving 100% compliance, hoping that either the regulator will not spot it, or if they do, the fine will be less than the cost of achieving the last 5%.

Clearly, the mechanism used for achieving compliance, especially where extensive use is made of checklists, may not adequately achieve a good level of security, even although it might achieve compliance. Assurance models which are based on standards and compliance goals may well provide assurance, but if the goals are not current, how useful will that really be? The same is true of external audit. Often, this is carried out some time after the year end is finished, merely compounding the lack of currency issue.

It is clear that the security environment in which companies operate today is a very hostile place indeed. It is also clear that in spite of spending serious amounts of money on security, many companies are not succeeding in keeping their

systems secure. Looking back at Figure 1 on page we can see how the tensions between all the actors can allow a misalignment of security goals, leading to a less complete level of security in the company. Equally, over-reliance on the use of checklists can give rise to a false sense of security.

In 2013, Duncan et al [26] proposed the use of an integrated security framework to ensure continuous compliance, assurance and security. Clearly, there needs to be an appetite for achieving security that starts right at the top of the company. Management need to take responsibility for setting the necessary goals and need to stay involved throughout the process of developing, installing and running proper security controls. There needs to be a proper focus on security expenditure. Adopting a risk assessment based approach to security can help focus management on where to spend money effectively.

It is obvious that with the inherent shortcomings of all these systems, a more effective approach is needed. A multi-tiered approach in each company is needed to achieve this goal. Management need to take full responsibility for driving a meaningful top down approach to information security. They need to set the declarative goals which the company must achieve, as well as defining the metrics necessary to measure performance. They should not devolve this task to, for example the IT department, but instead should take ownership of the task themselves. They should understand fully where their compliance obligations lie, and this should be at the heart of any goals they set.

The operational departments of the company must ensure the necessary steps, hardware and software are put in place to be able to meet those declarative goals set by management. The internal audit department are best placed to operate the assurance model, which calculates how well the operational measures that have been put in place are working towards meeting the declarative goals of management. Management can then have regular feedback on how well they are meeting their objectives. Thus the company can operate an effective real time assurance model which will ensure ongoing compliance, or at least provide early warning of any potential impending problems long before they become major disasters. Equally, if management have kept abreast of developments in the threat environment, they will be better placed to incorporate changes to help overcome new threats as they evolve, rather than finding out the hard way their security has been breached.

In this way, external auditors can carry out the audit function, knowing there is an effective internal system operating in the company. This will ensure that compliance will be more easily achieved, and the costs of external audit will be less onerous than the traditional approach of leaving compliance entirely to the auditors.

8. CONCLUSION

So, returning to the title, does compliance with standards, assurance and audit equal security? The answer is, of course, not necessarily.

The discussion above shows standards setters to be inevitably lagging the real world situation, effectively trying to manage a situation that was rather than is. Compliance is often reduced to a box ticking exercise due to the expense of using "real experts". Even assuming the writers of the checklist were expert enough, they would be unlikely to foresee and take into account the different environments and time periods for their checklist to be applied to.

We have seen how assurance is still a developing field and that audit is problematic, even in the highly regulated accounting environment where over a century of experience still leaves an imperfect system. IT audit is not only much more recent, but also far less regulated.

It is difficult to see how standard compliance alone, even if checked and verified, can give confidence about security in a world that moves on before the standard setters have arrived. An intelligent management approach would be to self-question its approach, asking — how committed are we to achieving security, how knowledgeable are we about the attack surface, how effectively do we set about achieving compliance, do we use a continuous assurance system, how expert and effective are our external auditors? Have management instilled a security ethic within the company? How well do we train our staff on using a secure approach at all times? Do we allocate sufficient resources towards security? Do we spend the allocated security budget effectively? Are we complying to the most appropriate standards? How well do these elements align with the goal of achieving security?

If a company can answer these questions positively, the answer might still be no, but at least managements' eyes are opened to the problems around them. An important goal is to make life difficult for the attacker at an affordable cost. Most attackers have an economic view of their victims' world. They want value for their efforts. If a company is proving too time consuming, or troublesome to get into, it is not too long before they move along to the next, and the next. There is still plenty of "low hanging fruit" ready to exploit.

9. REFERENCES

[1] H. o. L. S. C. o. E. Affairs. Big 4 Audit Firms Enquiry. Technical report, House of Lords Select Committee, London, 2013.

[2] R. Alexander, R. Hawkins, and T. Kelly. Security Assurance Cases: Motivation and the State of the Art. *www-users.cs.york.ac.uk*, pages 1–19, 2011.

[3] M. G. Alles, A. Kogan, and M. a. Vasarhelyi. Feasibility and Economics of Continuous Assurance. *Audit. A J. Pract. Theory*, 21(1):125–138, Mar. 2002.

[4] O. D. C. Alliance. Open Data Center Alliance Usage: Provider Security Assurance. pages 1–14, 2011.

[5] O. D. C. Alliance. Open Data Center Alliance Usage: Regulatory Framework. pages 1–25, 2011.

[6] O. D. C. Alliance. Open Data Center Alliance Usage: Security Monitoring. pages 1–9, 2011.

[7] O. D. C. Alliance. Open Data Center Alliance Usage: Service Catalog. pages 1–16, 2011.

[8] O. D. C. Alliance. Open Data Center Alliance Usage: Standard Units of Measure for IAAS. Technical report, 2011.

[9] D. S. Archambeault, F. T. DeZoort, and T. P. Holt.

The Need for an Internal Auditor Report to External Stakeholders to Improve Governance Transparency. *Account. Horizons*, 22(4):375–388, Dec. 2008.

[10] A. Baldwin, Y. Beres, and S. Shiu. Using Assurance Models to Aid the Rrisk and Governance Life Cycle. *BT Technol. J.*, 25(1):128–140, Jan. 2007.

[11] A. Beautement and D. Pym. Structured systems economics for security management. In *WEIS*, pages 1–20, 2010.

[12] Y. Beres and A. Baldwin. Model-Based Assurance of Security Controls. *Framework*, pages 1–7, 2008.

[13] BIAC and ICO. An International Business Commentary on the 2002 OECD Guidelines for the Security of Networks and Information Systems: Towards a Culture of Security. pages 1–24, 2003.

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

[15] BSI. The BS5750 Quality Management Standard, 2014.

[16] A. Cadbury. Cadbury Report: The Financial Aspects of Corporate Governance. Technical report, HMG, London, 1992.

[17] Cisco. Cisco 2010 Annual Security Report. Technical report, Cisco, 2010.

[18] Cisco. 2013 Cisco Annual Security Report. Technical report, Cisco, 2013.

[19] COBIT. *Executive Summary Framework*. 2007.

[20] J. Cohen, G. Krishnamoorthy, and A. M. Wright. Corporate Governance and the Audit Process. *Contemp. Account. Res.*, 19(4):573–594, 2002.

[21] M. Collinson. Behaviour, Interaction and Control of User Communities. *Communities*, pages 1–31, 2010.

[22] M. Collinson and D. Pym. Algebra and Logic for Resource-Based Systems Modelling. *Math. Struct. Comput.*, pages 1–57, 2009.

[23] P. S. S. Council. Data Security Standard Requirements and Security Assessment Procedures. Technical Report November, PCI Security Standards Council, 2013.

[24] CSA. Security Guidance for Critical Areas of Focus in Cloud. Technical report, Cloud Security Alliance, 2012.

[25] CSO. Cloud Standards, 2013.

[26] B. Duncan and M. Whittington. Developing a Conceptual Framework for Cloud Security Assurance. In *Cloud Comput. Technol. Sci. (CloudCom), 2013 IEEE 5th Int. Conf. (Volume 2)*, pages 120–125, Bristol, 2013. IEEE.

[27] ENISA. A Security Analysis of Next Generation Web Standards, 2013.

[28] K. Goertzel, T. Winograd, H. McKinley, L. Oh, M. Colon, T. McGibbon, E. Fedchak, and R. Vienneau. Software Security Assurance: A State-of-Art Report (SAR). pages 1–396, 2007.

[29] W. House. Administration Strategy on Mitigating the Theft of U.S. Trade Secrets. Technical report, White House, Washington DC, 2013.

[30] I. G. Institute. *Framework Control Objectives Management Guidelines Maturity Models*. 2007.

[31] ISACA. An Introduction to the Business Model for Information Security. Technical report, 2009.

[32] IsecT. Information Security Frameworks from "Audit" to "Zachman". Technical Report March, 2011.

[33] ISO.org. ISO/IEC 27000:2009 - Information technology – Security techniques – Information security management systems – Overview and vocabulary. Technical report, ISO.org, Geneva, Switzerland, 2009.

[34] Kaspersky. Threat Evolution Report for 2010, 2010.

[35] J. Mcgovern, J. Payne, and C. Watson. Software Assurance Maturity Model - Version1.0. pages 1–96, 2009.

[36] D. Midgley, R. Marks, and D. Kunchamwar. Building and Assurance of Agent-Based Models: An Example and Challenge to the Field. *J. Bus. Res.*, 60(8):884–893, Aug. 2007.

[37] R. Moeller. Managing internal auditing in a post-SOA world. *J. Corp. Account. Financ.*, 15(4):41–45, May 2004.

[38] P. G. Neumann. Computer-Related Risks. 1995. *Read. Addison-Wesley*, 1995.

[39] NIST. NIST Security and Privacy Controls for Federal Information Systems and Organizations. Technical Report February, Natioinal Institute of Standards and Technology, Gaithersburg, MD, 2012.

[40] OED. Oxford English Dictionary, 2014.

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

[42] N. Pham, M. Riguidel, and S. Naqvi. Security Assurances for Intelligent Complex Systems. *Proc. SPIE*, pages 1–12, 2007.

[43] T. F. R. Program and A. Management. FedRamp, 2014.

[44] PWC. Information Security Breaches Survey 2010 Technical Report. Technical report, PWC, London, 2010.

[45] PWC. UK Information Security Breaches Survey - Technical Report 2012. Technical Report April, PWC2012, 2012.

[46] S. Ramamoorti. Internal Auditing: History, Evolution, and Prospects. *Res. Oppor. Intern. Audit.*, pages 1–23, 2003.

[47] SOX. Sarbanes-Oxley Act of 2002, 2002.

[48] Trend. The Future of Threats and Threat Technologies How the Landscape Is Changing. Technical Report December, Trend Micro, 2010.

[49] Trend. A Look Back at 2011. Technical report, 2011.

[50] Trend. 2012 Annual Security Roundup: Evolved Threats in a "Post-PC" World. Technical report, Trend Micro, 2012.

[51] Trend and K. Wilhoit. WhoâĂŹs Really Attacking Your ICS Equipment? Technical report, 2013.

[52] Verizon. 2012 Data Breach Investigation Report: A study conducted by the Verizon RISK Team in cooperation with the United States Secret Service and Others. Technical report, 2012.

[53] G. T. Willingmyre. Standards at the Crossroads. *StandardView*, 5(4):190–194, 1997.

[54] S. A. Zeff. The SEC rules historical cost accounting: 1934 to the 1970s. *Account. Bus. Res.*, (2007):1–14, 2007.