Bow to the King (IV)? A new era for IT governance in South Africa

HF Theron & PGJ Koornhof
Department of Mercantile and Labour Law, University of the Western Cape
3350140@myuwc.ac.za; pkoornhof@uwc.ac.za

This work is based on the research supported in part by the National Research Foundation of South Africa for the grant, Unique Grant No. 99180. Any opinion, finding and conclusion or recommendation expressed in this material is that of the author(s) and the NRF does not accept any liability in this regard.

Abstract

Information Technology has become pervasive. No business can function efficiently without embracing the opportunities that dynamic IT practices present. A number of recent hacking and other IT related scandals illustrate that companies can’t afford to be blind to the risk that poor governance in this arena presents. IT is no longer part of doing business but business itself; and IT governance can no longer hover on the periphery of corporate culture. It speaks to the very core of modern corporate governance and risk management. In general, IT governance seeks to regulate and govern areas such as the electronic privacy of customers and employees, the productive use of IT in business; the protection of the online presence of business structures and minimum security standards. In the South African context, the 2009 King Report was notable for its inclusion of an entire Chapter dedicated to IT governance, one of the only self-regulatory codes to speak to it in such detail directly. Currently a fourth version of the report is being prepared, and its recently published draft shows a marked departure from previous versions, being a much more pared-down document. Significantly, the IT governance chapter has been removed, seemingly because principles related thereto have been disseminated throughout the draft report. This contribution assesses the state of IT governance before comparing King III to the Draft King IV Report. It is concluded that the move to less direct recommendations on IT governance is in line with foreign corporate governance codes, and that companies tend to adopt international standards in relation to this aspect.

Keywords

Information Technology Governance; King Report; Sustainable Business Practices; Information Security; Corporate Governance
1. Introduction

Information Technology has become so entangled in our daily lives that it is difficult to fathom a situation where it is not present, and businesses have become especially reliant on IT in the day-to-day running of their operations and in generating profit. (Boar, 2002) With the implementation of IT comes great power to expand and enhance business. (Enoch & Green, 1997) The impact of IT on the operation of firms has both strengthened the ability to monitor internal complexity, but also comes with new risks that did not previously exist, such as issues relating to information security. As such, if IT is properly managed, it simplifies business tremendously – but if not, it increases potential liability to the same extent. (Wixley & Everingham, 2010)

IT governance can be defined as a framework that supports the effective and efficient management of information resources to facilitate the achievement of corporate outcomes. The focus, as such, is on the measurement and management of IT vis-a-vis its associated risks and costs. (Naidoo, 2009; King III, 2009) It seeks to regulate and govern, *inter alia*, electronic privacy of customers and employees; the productive use of IT in the business structure; the protection of the online presence of business structures; protection against litigation; cyber security of business structures; the protection of intellectual property in its digital form and the management of electronic data and records in accordance with the law. (Giles, 2016)

Countries have differing approaches to corporate governance in general, with some adopting self-regulatory codes, others legislation, or a hybrid thereof. (Koornhof, 2013; Wixley & Everingham, 2010) In South Africa, the first notions of IT Governance specifically came to the fore in 2009 in the form of the King Report on Corporate Governance – at this stage already in its third iteration. (King III, 2009) The King Report on Corporate governance is a self-regulatory code researched and drafted by the King Committee on Corporate Governance. The three iterations of the King Report were published in 1994, 2002 and 2009 respectively. The jump from the second to the third King Report was of particular significance, not only due to the inclusion of principles relates to IT Governance, but also because it coincided with the introduction of the new Companies Act, 71 of 2008. (Naidoo, 2009) While it does not have legislative power, the King Reports are granted an elevated status through section 7 of the JSE Listing Requirements which requires listed companies to apply its principles and recommendations. (Wixley & Everingham, 2010) In developing jurisprudence, courts are also recognising its importance (See *South African Broadcasting Corporation Ltd and Another v Mpofu* [2009] ZAGPJHC 25).

Recently, the highly anticipated first draft of King IV was released for comment. It is expected to come into operation in November 2016. The draft report is bold in its undertaking, seeking to become the benchmark for good governance not only in public companies – its traditional field of application in practice – but also smaller ones, as well as the public sector. This was also a stated goal of King III, but the draft Report deals with this aspect in a far more express and nuanced manner both in
its explanatory introduction, its principles, and the general language used in it. The Draft Report also includes supplements for how the principles may apply differently in sectors such as municipalities, SMEs, NPOs, and SOEs. (King IV Sector Supplements, 2016) As such, the Report’s coming into effect may have far-reaching implications for what is seen as best practices and good governance all around.

While King III dealt with IT Governance in isolation, it has been stated that King IV seeks to approach and deal with this in a much more holistic manner given the pervasive effect of IT on business. (Draft King IV Report, 2016; Giles, 2016) This article seeks to consider IT governance in South Africa by looking at the current position in King III and comparing it to the new position proposed in the draft of King IV. This will be done in the light of developments both in foreign countries and international standards, along with critical commentary on King III itself. In doing so, a general overview of IT Governance principles and practices will be given, before moving on to a discussion of international instruments and the position in foreign countries. Subsequently, the focus will be moved to a critical comparison of IT Governance principles in King III and the draft King IV before concluding.

2. An Overview of IT Governance Practices and Principles

The general principle of IT governance is that management and the board should ensure that IT projects and systems are in line with overall objectives of the company, and that the risks and complexity related to these aspects are sufficiently managed. Given the great costs related to IT and the fact that mismanagement often creates systems that are unsuitable, principles of IT governance seek to assess whether or not related company processes are fit and proper in relation to their stated purpose. As such, individuals managing and measuring these processes should have the appropriate skill and awareness. (Wixley & Everingham, 2010; Cassim et.al, 2012)

Aspects relating to protection of information, the management of information and the protection of personal information processed by companies are considered key when assessing the sufficiency of IT governance practices. IT systems without proper, sophisticated, adaptive controls and security mechanisms can easily fall prey to cybercrimes, such as denial of service attacks and unauthorised access to sensitive information. (Naidoo, 2009; Ragan, 2013; Etsebeth, 2005) If ever there was doubt about the inherent importance of the above aspects, it has been wiped away clean by recent tech-scandals such as the hacking of Sony Pictures Entertainment and the Ashley Madison data breach. The 2014 Sony Pictures hack was a supposed retaliation by North Korea to the intended release of film ‘The Interview’ in the same year. The hack brought about a leak of approximately a hundred terabytes of sensitive information. (Betters, 2014) The Ashley Madison data breach of 2015 was a situation where a group set about leaking some twenty-five gigabytes of company data which it had gathered by hacking company servers. Ashley Madison is an enabling website for extramarital affairs. The data in question was extremely sensitive information of approximately thirty-seven million customers. This was
vastly damaging to the company, resulting in the company’s withdrawal from listing publicly with an intended $200 million initial public offering. Prominent members of society were also embarrassed as a result. (Thomsen, 2015; Krebs, 2015)

A variety of approaches to the implementation of corporate governance, of which IT governance is a subset, can be identified. As stated above, certain countries have adopted self-regulatory codes, while others have introduced legislative interventions – more informally referred to as soft law and hard law respectively. While some countries lean towards the former approach and others to the latter, most have effectively opted for a hybrid approach. Examples of foreign self-regulatory codes include the FRC Corporate Governance Code of the United Kingdom, the ASX Corporate Governance Principles in Australia, and the NYSE and NASDAQ Rules in the United States, as well as the OECD Corporate Governance Principles. Examples of legislation include the Sarbanes-Oxley Act in the United States along with several EU directives notably dealing with governance in the financial sector. Provisions relating to corporate governance are also found in the company legislation of Australia and South Africa. (Koornhof, 2013)

When comparing the above hard law and soft law, the most notable difference is the required standard of compliance, with the former generally adopting a strict application, and the latter comprising a more lenient and flexible approach. The so-called ‘comply or else’ standard is most effectively showcased through enactment of the US Sarbanes-Oxley Act in 2002. This is a strict and somewhat harsh response to a large array of corporate scandals in the USA during the early 2000s. All corporate entities are required to comply, with no exceptions. This model of corporate governance has been praised for holding all corporate entities equally accountable and critiqued in that it isn’t applicable all the time given that the scale of business carried out by companies may vary too considerably. (Hill, 2006; Koornhof, 2013)

In contrast to the above, the ‘apply or explain’ or ‘comply or explain’ standard is generally associated with self-regulatory codes. In essence, entities are given a set of standards, principles and/or recommendations to follow, but are not mandated to follow all of them necessarily. Instead, they may choose what is most appropriate to them and explain their non-compliance accordingly. This was the model applied by earlier versions of the UK Combined Code, the Dutch Tabaksblat Code, and the first two versions of the King Report. A newer variation on this standard, which was adopted by King III, is the so-called ‘apply or explain’ approach which expects companies either to apply the recommendations of the Code, or (in deviating from the recommendations) explain how they at least adhere to the overarching principles found in the Code. While still flexible in its application, it creates an additional layer of accountability whereby companies can’t simply disavow the principles of the Code. (Naidoo, 2009) In the explanatory memorandum to the draft of King IV it states that the flexible approach adopted in King III should be retained, but uses a slightly more onerous “apply and explain” approach, assuming that companies have complied with its principles as a point of departure. (Draft King IV Report, 2016)
3. International standards and foreign implementation

It is prudent to consider international best practices, given that principles related to IT governance have been around in some manner or form for quite some time, and have since been tabulated in various international standards. The most prominent ones will be discussed briefly below, along with the positions adopted in foreign countries.

a. Control Objectives for Information and Related Technology (COBIT)

COBIT is a widely used comprehensive framework which links business risks, needs for controls and technical issues associated with IT Governance. (Naidoo, 2009) Its framework provides metrics and maturity models to assess how the above issues are managed, and also identifies the associated responsibilities of business and IT process owners. (Mingay & Bittinger, 2002; Moeler, 2008; Marnewick & Labuschagne, 2011)

The newest iteration, COBIT 5, adopts five principles, and places an increased focus on processes, enterprise goals and enablers aligned with these principles. (ISACA, 2012) Principle 1 seeks to meet stakeholder needs by maintaining a balance between the realisation of benefits and the optimisation of risk and use of resources. Principle 2 seeks to integrate governance of enterprise IT into enterprise governance, holistically covering all IT-related functions and processes within the business from end to end. Principle 3 encourages the application of a single, integrated framework, noting that in the modern era there is a need to not only recognise but also align with other international standards. Principle 4 advocates a holistic approach to IT, noting that there are various ‘enablers’ which determine efficient and effective governance and management thereof, such as principles, policies frameworks; processes; organisational structures, corporate culture, and the skills and competencies of people within the business. Finally, Principle 5 seeks to separate governance from management, making a clear distinction between the two. In this regard, it states that: “Governance ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritisation and decision making; and monitoring performance and compliance against agreed-on direction and objectives.” On the other hand, it emphasises that “[m]anagement plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives.” As such, it distinguishes between the holistic, steering function of a board, including independent and non-executive directors, and the more specific day-to-day running of the business, dealt with by executive directors and management committees.

It should be noted that King III is considered to be most in line with COBIT, and the general sentiments about the division between governance and management are echoed therein. In fact, the King Report expressly notes that the implementation of COBIT could help achieve adequate IT governance. (King Report, 2009; Steenkamp,
2011) However, this reference was to COBIT 4.1, which used a different method to COBIT 5. It will be considered below whether this trend is followed in the draft of King IV.

b. ISO/IEC 38500

The ISO/IEC 38500 standard provides a framework with a view to assist those at the highest levels of organisations to understand and fulfil their legal, regulatory and ethical obligations in respect of the use of IT in their business structures. To this end, it places IT at a strategic level and looks at it from a demand standpoint, focusing rather on how IT can be used by a business than how it is implemented. Crucially, it places emphasis on top management’s behaviour in relation to IT governance, distinguishing clearly between the concepts of governance as a heightened and integrated degree of responsibility, and management, which is a more delegable and diluted responsibility. (ISO/IEC 38500:2015) Whereas COBIT adopts a more holistic view, this standard favours a more top-down approach. (Sylvester, 2011)

The standard prescribes three main tasks which directors should implement in governing the use of IT within their businesses, along with six overarching principles. The three tasks prescribed by ISO are the following: firstly, directors must evaluate the current and future use of IT in the company; secondly, directors must prepare and implement plans and policies to ensure that the use of IT meets the business objectives of the firm; finally, directors are to monitor the firm’s conformance to policies and plans as set out by management. The six principles advocated by the standard are: ensuring that IT responsibilities are clearly established; aligning corporate and IT strategy; ensuring that IT acquisitions and investments are made properly; ensuring that IT delivers its required performance; ensuring that IT conforms to all compliance requirements; and finally ensuring that IT policies and practices take human behaviour into account. (ISO/IEC 38500:2015; Harmer, 2015) Notably, while these principles prescribe what should happen, they do not always expressly state how, when or by whom it should be implemented. COBIT 5 recognises this aspect and uses it as a point of departure in aligning itself with the ISO standard. (ISACA, 2012)

c. The Calder-Moir Toolkit

In considering IT governance holistically, Calder submits that none of the above international standards provide full and comprehensive guidance, and consequently that other remedies must be sought. It is further noted that attempting to use these frameworks concurrently is also problematic given that they at times overlap and at others are at odds with one another. When firms try to reconcile these aspects, it may cause unnecessary wastage of resources and time, and essentially detracts from the main objective, namely the governance of IT. (Calder, 2008) To this end, the so-called Calder-Moir IT Governance Framework (colloquially known as the Calder-Moir Toolkit) was developed.
The toolkit is divided into six quadrants, arranged in a cyclical manner, relating to business strategy; risk, conformance and compliance; IT Strategy; managing change; maintenance of the information and technology balance sheet and, finally, operational management. The first three deal with planning in general, covering the processes for the establishing of directions, specifying constraints and decision-making. The last three in turn cover the development of new capabilities and the management thereof as well as the use of IT to deliver business products and services. (IT Governance Ltd, 2013)

True to its arrangement, the process of applying the toolkit is also cyclical, starting with business strategy and ending with operational management. Each of these quadrants is divided into three ‘layers,’ the inner (denoting key issues to be dealt with by the board), middle (the executive management’s responsibilities) and finally the outer layer (related to IT practitioners and delegated implementation). (Calder, 2008)

Essentially, the toolkit is a ‘meta model’ for the coordination of frameworks and the organisation of IT governance. While it often refers to the ISO standard, the toolkit is in itself intentionally devoid of such content in order for it to be able to be adapted to any particular strategy or corporate governance regime. (IT Governance Ltd, 2013)

d. Implementation of IT Governance in other countries

As already mentioned, most countries use some kind of hybrid system when it comes to corporate governance in general, with certain aspects covered by legislation and others by self-regulatory codes. In the United States, legislation such as Sarbanes-Oxley largely deals with financial matters, with more nuanced aspects of corporate governance for listed companies being dealt with in the listing requirements of stock exchanges. Both Section 303A of the NYSE Listed Company Manual and the NASDAQ Marketplace Rule 5600 Series, which state the corporate governance standards for their respective exchanges, are wholly silent on the issue of IT governance. However, the NYSE Corporate Governance Guide does mention that the best practices for listed companies would be to adopt COBIT (Rosenblum et al, 2014). The United Kingdom position is practically the same, with neither the 2006 Companies Act nor the 2014 Corporate Governance Code providing specific guidance. The 2015 OECD Principles are similarly silent. It is submitted that a possible reason why most country-specific codes are silent on the subject of IT governance is as a result of multinational corporations which, given that they operate globally, likely adopt international standards for such issues, rendering it somewhat moot.

The only notable country to adopt its own standard was Australia, with the publication of AS8015 in 2005. The standard’s framework provides for six principles of good IT governance, namely: establish clearly understood responsibilities for ICT, plan ICT to best support the organisation, acquire ICT validly, ensure that ICT performs well, whenever required, ensure ICT conforms with formal rules and
ensure ICT respects human factors. Furthermore, the standard denotes that governance responsibility is subject to delegation to “senior managers, technical specialists, vendors and service providers.” It ultimately formed the backbone of the ISO/IEC 38500 standard, which has effectively replaced it. (Ramin Communications, 2016)

4. Comparing King III to the draft King IV Report

The principles of IT governance in King III are found in Chapter 5 and seek to highlight the most salient aspects for directors to focus on. Due to the broad and ever-evolving nature of the topic, it does not try to be the definitive text on the subject but rather to create a greater degree of awareness at board level.

King III states that pursuant to the digital nature of business conducted today and the vast automation reform of enterprise, information technology has become such an integral part of the business model in South Africa that there is a need to regulate it distinctively as it forms part of the larger corporate structure. Specific notice has been taken of how IT is and can be used as a ‘strategic asset’ to gain a competitive edge in the marketplace. One of the key aspects that King III sought to rectify is the perception that IT governance is ‘the IT department’s responsibility’ and not that of top-tier management. (Steenkamp, 2011)

Chapter 5 provides 7 overarching principles, namely that: the board should be responsible for IT governance; IT should be aligned with the performance and sustainability objectives of the company; the board should delegate to management the responsibility for the implementation of an IT governance framework; the board should monitor and evaluate significant IT investments and expenditure; IT should form an integral part of the company’s risk management; the board should ensure that information assets are managed effectively; and finally, the risk and audit committees should assist the board in carrying out its IT responsibilities. Along with these seven principles are 48 recommendations that outline how this should be enacted. Some of the notable specific recommendations include that companies should adopt an IT Charter and that a suitably qualified Chief Information Officer should be appointed.

King III speaks to IT governance in a very concise manner and has been criticised for being ambiguous at times, with specific reference to the potential uncertainty and confusion that may arise when determining whether a specific principle has been complied with. Businesses wishing to satisfy compliance have therefore sought assistance from international standards and compliance toolkits. (Etsebeth, 2010) While these aspects are mentioned in Principle 5.6, King III has been criticised for failing to sufficiently deal with aspects related to information security and information privacy. (Ragan, 2013) While this is a criticism of the Report itself, it should be noted that legislation such as the Protection of Personal Information Act, 2013 and the Promotion of Access to Information Act, 2000 may to a certain extent rectify this situation in relation to information privacy. Information security is also,
Turning to the draft King IV Report, the text also does not pretend to be a definitive one in relation to IT governance. Nevertheless, an increased emphasis on information technology is placed in the draft’s foundational concepts, describing its advent as ‘the fourth industrial revolution’. Additionally, recommended practices of principles tangentially related to IT can be identified. Firstly, it is noted that organisations are to engage with stakeholders in new ways, of which digital communication platforms such as social media form a part. This is reiterated in Principle 5.1. Secondly, firms are required to adopt a ‘new perspective of risk’ since risks are evolving, due to globalisation and increased connectivity. Thirdly, a key aspect which is raised is the fact that more categories of jobs will be automated. The industries of robotics and artificial intelligence will thus become more prominent, forcing organisations to consider the effect of this on business, employees and larger society. Fourthly, its conception of the role of the governing body entails managing technology and information in a manner that supports the organisation’s defining core purpose and setting out and achieving strategic objectives. Finally, Principle 3.4 advocates that responsibilities for functional areas including technology and information be managed with appropriate experience, be appropriately resourced and sufficiently defined so as to create certainty. While the phrases ‘information security’ and ‘information privacy’ are not expressly mentioned, it is submitted that, when holistically analysing the text, they are seen as priorities.

Principle 4.2 of the draft report reiterates that the governing body should govern technology and information in a way that supports the organisation in defining its core purpose and to set and achieve strategic objectives. Seven recommended practices are stated in relation to this. These practices are that: the governing body should provide strategic direction for management in respect of IT; the governing body should approve policy that articulates strategic use and direction of IT; that such policy should adopt appropriate standards to give effect to strategy; the governing body should delegate to management the responsibility of implementation of policy on IT, not only in respect of day-to-day activities, but also in relation to medium to long-term decision-making, activities and culture in general; the governing body should oversee the adequate and effective implementation of technology and information management; the governing body should oversee the management of cyber-security risk; the governing body should periodically carry out review of the adequacy and effectiveness of the organisation’s technology and information function, and finally that there should be disclosure and reporting at each stage of implementation of IT policies. Essentially these principles encompass the governing body’s authority to delegate, oversee and review the governance of IT in the business structure. It is retains the concise and summarised nature similar to that of Chapter 5 in King III, and it is submitted that potentially the same problems in interpretation and implementation may arise.
It is submitted that what King IV seems to have done is attempt to incorporate into its text an approach similar to that of the Calder-Moir Toolkit. Seemingly it takes the most prominent best practices from each of the international standards and incorporates them in an effort to secure adequate and effective IT governance. Similar to COBIT 5, the draft King IV seemingly also makes a more pronounced distinction between aspects related to ‘governance’ and that of ‘management,’ opting for the delegation of responsibility with regard to implementing IT policies and process to management, while the governing body should be more involved in holistic policy development and the subsequent oversight of management. Whereas King III was influenced by the principles of COBIT 4.1, the drafters of the King IV appear to have placed their reliance on the provisions of COBIT 5.

Mervyn King, the former head of the King Committee, advocated that ‘a company’s board must be directly involved in IT governance’ (Steenkamp 2011). Where IT governance has been shown to be most effective is when it is governed by the board itself in line with the ISO standard and not that of COBIT. (Hardy, 2008) However, it is trite that members of the board cannot concern themselves with every single decision to be made on a day-to-day basis and as a whole may not always have the prerequisite skills and knowledge to make the right call. Milner criticises the lack of references in the draft to a Chief Information Officer or IT Steering Committee as one that could be problematic in this light. (Milner, 2016) Visser in turn argues that the importance of social media is understated, and that this should be emphasised. (Visser, 2016) Everingham also points out in his commentaries on the draft that in implementing Principle 4.2 it may prove difficult to assess return on investment in technology and information systems. As such, he notes that there should be a careful post-implementation audit of the actual delivery provided by such investment against what may have been promised. (Everingham, 2016) These lacunae may create a situation where organisations who are new to IT governance and do not view the Report in context with international instruments may inadvertently create inappropriate structures in comparison to what was specifically prescribed by King III. Notwithstanding these commentaries, the reaction to the draft has been largely positive. An alternative point of view to this would be that the Report shies away from using a check-list approach, rather opting to provide organisations freedom in determining how best to implement IT governance in their unique environment. It is submitted that one must take into account the nature and logistics of modern day business, to which end an amalgamated approach will be most beneficial. Seemingly, the draft King IV adopts such an amalgamated approach.

5. Conclusion

The draft of King IV recognises IT as an integral part of nearly every aspect of corporate governance, not merely as a separate consideration placed within a standalone chapter. Also, added weight is given to the value of data and data structures, although they are not considered at length. Although King III deals with IT governance, it has been criticised as being vague and convoluted in its approach. This led organisations to consider the implementation of compliance toolkits which,
although rendering a satisfactory result, derogated from the King Code’s direct utility in respect of IT governance in a South African context. To this end the drafters of King IV have seemingly attempted to incorporate the strength of compliance toolkits by taking the best of each international standard and applying it throughout King IV.

The trend in most foreign countries has been to do away with any specific principles relating to IT governance, possibly in recognition of the fact that far better specialised instruments exist, and that it is unnecessary to reinvent the wheel in this regard. It can therefore be asked why the draft features any specific recommendations at all. It is submitted that a potential answer to this is that, given the isolated nature of the South African economy and the fact that King IV seeks to apply to a variety of sectors, at least some principled guidance may initially be required. While it can be stated that the provisions of the draft are largely a step in the right direction, it is submitted that in future, more – which in this particular instance would be less – can possibly be done in order to align the South African approach to IT governance with that of the rest of the world. Kneel down to the King? Possibly not yet. However, a respectful nod seems warranted.

6. References

Books


Journal Articles

Etsebeth, V. (2010) “King III on IT Governance: making good, making promises or making trouble” De Jure
Hill, JG (2006) Regulatory Responses to Global Corporate Scandals, University of Sydney Legal Studies Research Paper No 06/35
Koornhof, P (2013) “An overview of recent changes to Corporate Governance frameworks as
it pertains to Executive Remuneration” Speculum Juris 2013(1)
Marnewick, C & Labuschagne, L. (2011) “An Investigation Into the Governance of
Information Technology Projects in South Africa” JIPM 29:6
XIIX:4
compliance with the King III Report’s requirements for good IT governance” SA Journal for
Accountability and Auditing, Vol. 11
Van Solms, B. & Von Solms, R. (2005) “From information security to ... business security?”

Case Law

South African Broadcasting Corporation Ltd and Another v Mpofu [2009] ZAGPJHC 25

Domestic Legislation

Companies Act, 2008
Electronic Communications and Transactions Act, 2002
Promotion of Access to Information Act, 2000
Protection of Personal Information Act, 2013

Foreign Legislation

Companies Act, 2006 (c46) [England]

Online Sources

Corporate Governance Principles and Recommendations (the Third Edition) (2014), ASX
Thomsen, S. (2015) “Extramarital affair website Ashley Madison has been hacked and attackers are threatening to leak data online” available at http://read.bi/1HLXHUC [Accessed 14/06/2016].