CGF RESEARCH INSTITUTE (PTY) LTD
Corporate Governance Framework®

www.dqs.co.za

ARTICLE

Article issued by CGF Research Institute and DQS South Africa

Johannesburg
17 February 2014

OBLIGATION TO PROTECT CUSTOMER'S INFORMATION

There have been a number of high profile cases involving companies who have been accused of not implementing adequate measures to protect the information contained within their management systems. And whilst some countries across the globe have set tough regulations for companies to follow, many companies still pay scant regard in this respect. Indeed, as the fines and penalties are becoming more onerous, it may not necessarily be the fines that prompt companies to act more diligently when pondering greater measures to protecting the information within their systems. The reputational damage caused to companies accused of the underlying poor governance and inadequate data and information security is huge. The reputational damages and loss of customer's confidence caused can run into millions of lost revenue as customers seek other companies who are committed to protect their information.

Customers become very concerned -- and rightly so -- when their personal information such as credit card details, passwords, physical addresses, identity numbers and so forth become compromised by those whom were entrusted with such information in the first place. Not that long ago, Sony Corporation were accused for allegedly losing one hundred and one million customer records, and that as many as ten million customers may have had their credit and debit cards compromised as a result. Due to the extent of the potential knock-on effects of cyber criminality, the FBI also became involved.

And as expected, financial institutions have also not been left untargeted in this regard. The most well-known cases in recent times involve the HSBC, Zurich Insurance and Barclays. In the case of HSBC, in 2009 the bank was fined by the Financial Services Authority (FSA) for £3million for allegedly losing one hundred and eighty thousand customer files containing personal information. In the FSA's report, the bank was accused of being "careless with personal details which could have ended up in the hands of criminals." Again, the case of Zurich Insurance was not that much different and the FSA fined them £2.27million for allegedly losing the personal details of forty six thousand customers. Zurich was accused by the FSA saying that "Zurich UK let its customers down badly"; and the CEO of Zurich -- Stephen Lewis -- reportedly said, "this incident was unacceptable."

Of course, these *incidents* continue, and they will continue as long as companies remain relaxed about protecting their data and customer's information. The only way to rectify this increasing trend is by implementing the necessary (and appropriate) information security systems and staying vigilant against any possible breaches and attacks in this area. Most recently, Barclays have also been accused of alleged theft involving the sell-off of about twenty seven thousand customer files containing their confidential information. Notwithstanding any of these cases, the systems and controls to protect information -- and which is a requirement for proper record management governance -- appear in many cases to be weak, and no doubt in smaller companies may be non-existent.

As more breaches and violations of information protection occur, companies will bear the consequences attached to their failure to implement robust Information Security Management Systems (ISMS). Information security is one of the central concerns of the modern organisation and through ISO 27001 for example, it informs organisations how to operate and protect information within its structures.

It is critical for customers -- in particular -- to know and trust that companies will protect their information and that the necessary assurances are provided through its compliance with ISO 27001. Undoubtedly,

the main drivers for security and the protection of information are; increased globalisation, government directives, terrorist activities and threats from hackers. As more global companies spread their operations to build markets in South Africa for example, an additional supply chain requirement for doing business will also depend upon ISO 27001 being a prerequisite for doing business.

In closing, the Protection of Personal Information Act (POPI) which was signed into South African law on 26 November 2013, will significantly impact on the way in which companies collect, store, process and disseminate information from and to clients, employees and customers. POPI promotes the protection of personal information processed by public and private organisations and it aims to introduce certain information on protection principles to establish minimum requirements for the processing of personal information. If an organisation processes personal information -- (i.e. collects, receives, records, organises, collates, stores, updates, modifies, retrieves, alters, consults, uses, disseminates, distributes, merges, links, erases or destroys) -- it is important to consider the implications when the systems, processes and controls are not adequately in place to fulfil the requirements to protect customer information.

Following the examples of the FSA's fines given to HSBC and Zurich Insurance, POPI also has stringent requirements as well as substantial penalties for those who transgress. Any person or organisation who contravenes the provisions of POPI could face a prison sentence and fines of up to R10million. And if this was not enough, POPI also allows individuals to levy civil claims so there is also the possibility of additional financial losses.

ENDS

Words: 854

ABOUT ISO 27000

The ISO 27000 family of standards offers a set of specifications, codes of conduct and best practice guidelines for organisations to ensure strong IT service management. Of primary interest to information security are ISO 27001, ISO 27002 and ISO 27005.

ISO 27001 is a technology-neutral, vendor-neutral information management standard (it is not a guide). Of the three parts to IT security governance, ISO 27001 offers the specification – a prescription of the features of an effective Information Security Management System (ISMS).

As the specification, ISO 27001 states what is expected of an ISMS. This means that, in order to receive certification or to pass an audit, a company's ISMS *must* conform to these requirements.

While ISO 27001 offers the specification, ISO 27002 provides the code of conduct – guidance and recommended best practices that can be used to enforce the specification. ISO 27002, then, is the source of guidance for the selection and implementation of an effective ISMS. In effect, ISO 27002 is the second part of ISO 27001.

Just as ISO 27002 provides a set of guidelines for best practice in implementing an ISMS, ISO 27005 provides guidelines for risk management. As part of constructing a suitable and secure information management system, a company *must* assess the risks to its information and be prepared to mitigate these risks.

More information regarding CGF can be found at www.cgf.co.za
More information regarding DQS can be found at www.dqs.co.za

For further information contact:

CGF Research Institute (Pty) Ltd
Terry Booysen (Chief Executive Officer)
Tel: 011 476 8264
Cell: 082 373 2249
E-mail: tbooysen@cgf.co.za

DQS South Africa (Pty) Ltd
Jeff Hollingdale (Associate)
Tel: 011 787 0060
E-mail: jeffh@dqs.co.za