2014 To Bring A ‘Storm Of Change’ In InfoSec Compliance, Says IT Governance

Submitted by: 80:20 Communications Limited
Thursday, 12 December 2013

Ely, England, 12 December 2013 – The coming year will bring a ‘storm of change’ in information security compliance, creating fresh challenges for board directors, CIOs and business owners seeking to ensure business resilience, says IT Governance Limited (http://www.itgovernance.co.uk/).

Alan Calder, Founder and Executive Chairman of the global cyber security services provider, says: “A raft of new standards and regulatory controls are about to be launched in response to the rising tide of infosecurity threats. While these measures are to be welcomed, organisations will have their work cut out in preparing themselves to achieve compliance.

“The UK government has announced its intention to back a new kite-mark standard for cyber security, with further details promised in early 2014. Around the same time, the European Commission will unveil a new directive on data privacy, while the Obama Administration will introduce a nationwide cyber security framework in the United States. Add to these changes the multiple compliance challenges arising from recent updates of standards, such as ISO 27001 and PCI DSS, and you quickly have a considerable governance task in terms of planning, resourcing and training.”

IT Governance highlights five forthcoming changes in particular as requiring urgent attention from senior management:

• The UK government’s proposed kite-mark standard for cyber security, which is intended to provide a common set of guidelines for managing cyber risks and help stimulate the adoption of good cyber practices among businesses. Following an initial announcement by the Department for Business, Innovation and Skills on 26 November, further details and a formal launch are promised by the Department in early 2014.

• The EU’s draft General Data Protection Regulation (GDPR), which will supersede the EU Data Protection Directive, is expected to be formally adopted in mid-2014 and to take effect in 2016 after a transition period of two years. The GDPR aims to harmonise data protection regulations throughout the EU, strengthen online privacy rights and boost Europe’s digital economy.

• Version 3 of the Payment Card Industry Data Security Standard (PCI DSS), released last month, which requires merchants to be far more structured in their approach to issues including penetration testing and staff awareness training.

• The latest update to the ISO 27001 best practice information security standard, ISO 27001:2013, which was issued in October 2013 and is expected to progressively come into force during 2014 and 2015.

• President Obama’s planned cyber security framework for private companies and infrastructure networks, which is planned for finalisation in February 2014.

Calder says: “For any organisation working nationally or internationally, there is every chance of being affected by some or possibly all of these forthcoming changes. Therefore, as senior managers

contemplate the coming year, they have little time to waste in reviewing their current governance processes and preparing for the new requirements soon to arise.

“While the new measures are varied in nature and application, a common thread running through them is the need for a best practice approach to managing data assets. ISO 27001 helps address some of the challenges that are typical for data protection and PCI DSS compliance and enables the adoption of a holistic approach to security. Moreover, it supports a risk-based approach to security and facilitates the governance aspect which is so crucial. We therefore see compliance with ISO 27001 as the fundamental enabler to help organisations meet their regulatory obligations and the expectations of their customers.”

- Ends -

FOR FURTHER INFORMATION
80:20 Communications
Tel: 01483 447380
Marc Cornelius, mcornelius@8020comms.com
Susie Lunt, slunt@8020comms.com

NOTES TO EDITORS:

IT Governance Ltd is the single-source provider for books, tools, training and consultancy for IT governance, risk management and compliance. The company is a leading authority on cyber security and IT governance for business and the public sector. IT Governance is ‘non-geek’, approaching IT issues from a non-technology background and talking to management in its own language. The company’s customer base spans Europe, the Americas, the Middle East, South Africa and Asia. More information is available at: www.itgovernance.co.uk.