

IT Governance welcomes cyber resilience action plan launched by the Scottish public sector

ELY, CAMBRIDGESHIRE, UNITED KINGDOM, November 20, 2017 /EINPresswire.com/ -- IT Governance has hailed the recent launch of the Scottish public-sector's cyber resilience action plan as a progressive step forward to address the multitude of information security challenges that traditionally exist in public sector organisations.

Alan Calder, CEO and executive chairman of IT Governance, said: "We are pleased that the Scottish government has taken this crucial step forward in the field of cyber security and governance by choosing to play a true leadership role in business and society at large.

"The persistent and severe threat of large-scale cyber attacks and the dire consequences of being subject to an attack require all businesses to urgently put in place a cyber resilience programme that will help them to not only protect their information but also respond to and recover from such attacks.

"It is heartening to see that alignment with ISO 27001 and the Cyber Essentials scheme are acknowledged as leading examples of cyber security, and that the government has recognised that effective business continuity management makes up an essential part of a comprehensive cyber resilience programme."

The action plan sets out the 11 key actions that the Scottish government, public bodies and key partners will take up to the end of 2018 to enhance cyber resilience in Scotland's public sector.

[Read more about the Scottish public-sector action plan and requirements >>](#)

All Scottish public bodies must implement minimum cyber risk governance arrangements by the end of June 2018, and adopt independent assurance of critical cyber security controls by the end of October 2018 through Cyber Essentials certification.

In line with cyber security best practice, organisations should adopt effective cyber incident response plans and staff training and awareness, and start reporting against a set of newly developed guidelines from the end of June 2018.

A set of best-practice guidelines (view draft) has been developed to support the action plan. Scottish public bodies should pay attention to these guidelines when providing governance statements and certificates of assurance under the requirements set out in the Scottish Public Finance Manual.

The Scottish government has listed a range of existing standards, guidelines and controls that can contribute to increased cyber resilience, including ISO 27001, Cyber Essentials and the Payment



Card Industry Data Security Standard (PCI DSS).

IT Governance can help Scottish public-sector organisations align their cyber resilience strategies with international best practice. Please visit our [website](#) for more information about our [cyber resilience products and services](#), or email servicecentre@itgovernance.co.uk or call +44 (0)333 800 7000 to get in touch with our consultancy team.

- Ends -

NOTES TO EDITORS

IT Governance Ltd is the single-source provider of books, tools, training and consultancy for IT governance, risk management and compliance. It is a leading authority on data 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. Its customer base spans Europe, the Americas, the Middle East and Asia. More information is available at www.itgovernance.co.uk.

Mihaela Jucan
IT Governance Ltd
00448450701750
email us here

This press release can be viewed online at: <http://www.einpresswire.com>

Disclaimer: If you have any questions regarding information in this press release please contact the company listed in the press release. Please do not contact EIN Presswire. We will be unable to assist you with your inquiry. EIN Presswire disclaims any content contained in these releases.

© 1995-2017 IPD Group, Inc. All Right Reserved.