

Bristol, UK (PRWEB) 2nd November 2011



UK firm, Infogov Launches iGRC™ Website

UK firm, Information Governance Limited launched its integrated governance, risk and compliance website today – www.informationsecurityprotection.com.

Their iGRC™ capability combines Infogov's leading Proteus® Enterprise information security management system with network security related sensor technologies via an interface entitled GRCiP – the open governance, risk and compliance inter-operability protocol.



The iGRC Consortium project manager, Mike Popham said "To sustain a consistently high level of security in complex ICT infrastructure, processes and management must all operate within a single governance, risk and compliance control framework able to adapt swiftly to current and anticipated threats and vulnerabilities." "The Requirements Builder available via the 'Find Out More' page on www.informationsecurityprotection.com will aid firms define their approach to enhancing network security.", he added.

Value Proposition

Target organisations for this technology will be those supporting critical national infrastructure, e.g. verticals and industries with significant brand/reputation risk.

The primary value proposition is that iGRC™ provides:

- an insurance policy for CEOs wanting to assure the integrity of critical controls and measures to maintain low probability of occurrence of high impact risk events
- calibration of risk profiles in the round and validation of controls and measures baselines (risk event occurrence implies security baseline assessment is flawed)
- automation capabilities of control status and threat level change

True Situational Awareness

iGRC™ brings true situational awareness into the information security space. Proteus® in its iGRC™ configuration coupled to network sensors via the open GRCiP protocol will enable recognition of threats at an early stage through the automation of control status and threat level change and the taking of measures to avoid it. The iGRC Consortium is aware of the cultural aspects of situational awareness on organisations, particularly as it can be adopted and employed by anyone, including CIOs and CSOs on behalf of operations and Executive Boards alike.



The Consortium considered a dynamic and integrated approach to GRC practices because of:

- the speed and frequency of new regulatory requirements
- a need to enhance, enforce and reinforce codes of conduct
- complex operations having limited ability for consolidated reporting
- manual processes needing to be automated to avoid non-compliance
- knowledge gaps in agile risk and compliance operations
- board-level reporting lagging operational events and detail

A wide range of sensors are involved such as:

- host based intrusion detection, vulnerability assessment, configuration and policy compliance, database logs, web site logs, file accesses
- hosts for penetration testing, email scanning, spam filters
- network intrusion detection and prevention, netflow, firewall/router/other network devices logs
- access and identity for successful or failed logins, new users, deleted users, privilege escalation, bio-metric identities
- web site vulnerability detection (cross site scripting, SQL injection etc), pages visited, referred from
- end-point monitoring such as permitted user activity, not permitted user activity, data leakage monitoring, USB usage monitoring and reporting
- anti-virus, anti-phishing, malware detection
- applications - most keep audit logs of activity, and
- others such as event and audit log collection for operating systems, infrastructure and applications

All of these sensor types feed the GRC management suite that includes utility such as online compliance and gap analysis, business impact analysis, risk assessment, business continuity, incident management, asset management, organization roles, action plans, document repository and document dissemination, all from a risk management perspective.

For an explanation of iGRC™ please see:

[http://en.wikipedia.org/wiki/Governance, risk management, and compliance.](http://en.wikipedia.org/wiki/Governance,_risk_management,_and_compliance)

Supporting any standard the Proteus® GRC compliance questionnaire library contains such standards as: BS ISO/IEC 27001, ISO20000, ISO9001, PCI DSS, ISF SOGP, CobiT, BS ISO 38500, Sarbanes Oxley, HIPAA, BS 10012, Data Protection Act (DPA), Freedom of Information Act (FOI), Physical Risk, Caldicott, BS25999, and Civil Contingency Act. Licensed by the BSI for their standards as appropriate, renewal or development of internationally derived regulatory frameworks, including National Institute of Standards and Technology (NIST), can be lifecycle supported to order.

About the iGRC Consortium

Lead partners, Information Governance Limited are supported by HP Enterprise Services (previously EDS), Assuria and Nexor, and the Universities of Cranfield, Loughborough and London (Birkbeck College).

Contact for Information

Mike Popham, iGRC Consortium Project Manager
Director, Information Governance Limited
+44(0)797 650 4897
mike.popham@infogov.co.uk
http://twitter.com/popham_infogov - My News
<http://www.informationsecurityprotection.com>