

All-in-One Third Party Information Assurance

Setting the Standard for Third Party Information Assurance

Businesses of all sizes use outsourced services to support their critical business functions. While businesses can outsource sensitive data, processes and services, they can not outsource responsibility for the associated risk. To manage this risk and meet regulatory requirements, businesses must evaluate carefully the security controls of their service partners.

1 - Our approach

Due diligence requires social intelligence

To manage risk and meet regulatory requirements, businesses must gather information, track issues, and model the potential impact on the organization. It is impossible to make the right decisions when intelligence is in silos. Success depends on combining the intelligence of key stakeholders such as vendor management, contract management, information security, disaster recovery and business continuity planning, and physical security.

Due diligence is about going green

Most businesses meet different regulations by slicing risk management into different silos. Business can make better use of their resources, and improve their risk management, by combining the risk management effort across different silos.

All-in-One Third Party Information Assurance captures the commonality and synergy between different regulations (and the differences), and allows businesses to recycle the controls and policies developed for one regulation to meet new mandates.

This approach works because the requirements of different regulations are broadly similar and can be combined into a coherent whole. For example, a business that is ISO 27001 certified is likely to have already implemented many of the policies, practices and controls of PCI DSS.

2 - All-in-One Information Assurance

All-in-One Third Party Information Assurance is a powerful platform for risk and compliance intelligence that highlights risk issues with outsourced service providers.

Building blocks

The heart of All-in-One is a library of building blocks that evaluate different aspects of risk.

Each building block represents a single aspect of risk management. Building blocks gather metrics on the business' performance and compliance. Building blocks also measure the maturity level of the organization, to understand the evolution and implementation of policies, procedures and controls.

All-in-One Third Party Information Assurance

Templates

The building blocks are arranged into templates that represent coherent sets of risk management requirements. The building blocks allow the templates to be rapidly customized to the specific needs of the organization.

Example templates include:

- The Agreed Upon Procedures (AUP) of the Shared Assessments Organization (see <http://sharedassessments.org/value/aup.html>). These cover risk management, information security policy, organization of information security, asset management, human resources security, physical and environmental security, communications and operations management, access control, information systems acquisition, development and maintenance, incident and event management, business continuity management, compliance and privacy.
- PCI 1.2 PCI DSS 1.2 of Payment Card Industry
- Protection profiles based on NIST SP800-53 revision 3, with mappings to CobiT and ISO 27002.

Assessments

All-in-One provides easy-to-use on-line forms to capture risk management information. Different types of assessment (such as different service providers) can be grouped to reflect the structures in use by the organization.

Analysis

All-in-one provides powerful analysis capabilities. Key capabilities include:

- Consolidation that shows what really matters to the organization, with priorities and drill-down to the detail. This shows the forest and the trees on the same report.
- Rule-based analysis using an expert system to identify issues and risk, make recommendations, and set priorities.
- Reports which provide a view of the data specific to different regulations and standards, including:
 - AUP Agreed Upon Procedures
 - ISO 27002 information security standard
 - Defense in Depth (protect-detect-respond-sustain dimensions, and people-technology-process dimensions)
 - PCI DSS 1.2 of Payment Card Industry
 - SANS – 20 Critical Controls for Effective Cyber Defense (Priority 1, Priority 2)
 - Data leakage/Lost Protection
 - Protecting the confidentiality of Personally identifiable information (PII)
 - COSO Internal Control Framework
 - CobiT Control Objectives for Information and related Technology

As well as delivering management reports, all information can be exported to Excel or XML data.

All-in-One Third Party Information Assurance

Education and training

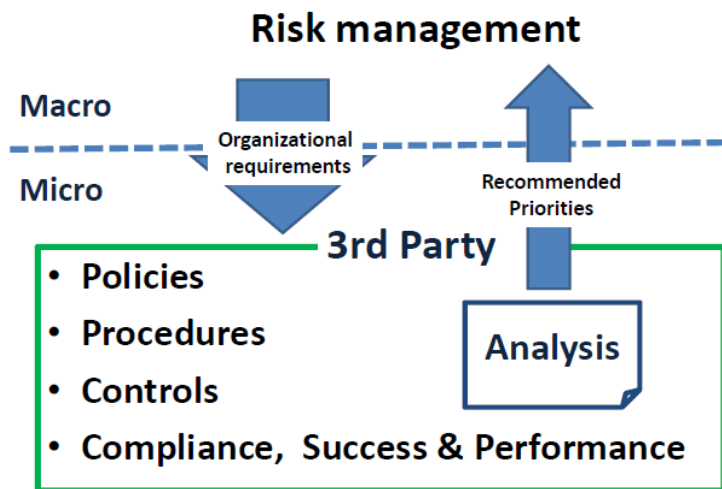
All-In-One is supported by a comprehensive package of education and training.

We offer a Quick Start programme, with a free initial workshop, followed by a Proof of Concept, and detailed implementation planning.

We offer assessment services, to create an inventory of your IT systems, and a risk-based classification of vendors and suppliers.

Through our partner Security Horizon, we offer training in the Information Security Assessment Methodology (ISAM). This provides a structured framework for the evaluation and communication of information assurance priorities to decision makers, and is an excellent approach for ensuring the take-up of information assurance initiatives.

3 - Summing Up



All-in-One Third Party Information Assurance delivers greater internal efficiencies and a standard methodology for engaging with industry partners. Being part of the Shared Assessments initiative gives even greater benefits, as financial institutions and service providers devote more resource to service delivery, and less to redundant security assessments.

How to buy

All-in-One Third Party Information Assurance is available either as a hosted service, or as installable software. Three All-in-One products are offered: Named user, monthly contract; Enterprise hosted, annual contract; Enterprise onsite, i.e. supply software for single installation onsite, perpetual license purchase plus annual maintenance.

Please contact us at sales@michelgodet.com to discuss how we can help your organization.

About Michel Godet and Metrici

Michel Godet is an independent consultant specializing in risk management, compliance, assurance protection strategy and information security. Metrici (<http://www.metrici.com>) provide Metrici Advisor, a web-based assessment tool which powers the All-in-One product.