

## Business Assurance for the 21st Century



14/07/2011

Navigating the Information Assurance landscape

## AUTHORS

NAME	AFFILIATION
Niall Browne	Shared Assessments Program
Michael de Crespigny	CEO, Information Security Forum (ISF)
Jim Reavis	CEO, Cloud Security Alliance
Kurt Roemer	Payment Card Industry (PCI) board of advisors
Raj Samani	Common Assurance Maturity Model (Camm)
Marc Vael	Chair of the Cloud Task Force and Chair of the Knowledge Board, ISACA

# TABLE OF CONTENTS

- 1 INTRODUCTION .....3**
  - 1.1 PURPOSE..... 3
  - 1.2 AUDIENCE..... 3
  - 1.3 APPROACH..... 3
- 2 CURRENT APPROACHES TO ASSURANCE.....4**
  - 2.1 A COMPLICATED ENVIRONMENT..... 4
  - 2.2 A GLOBAL PERSPECTIVE..... 4
- 3 KEY STAKEHOLDERS .....6**
  - 3.1 PCI-DSS..... 6
  - 3.2 CLOUD SECURITY ALLIANCE ..... 6
  - 3.3 SP800..... 7
  - 3.4 ISO / IEC 27xxx ..... 7
  - 3.5 SHARED ASSESSMENTS PROGRAM..... 9
  - 3.6 COBIT ..... 9
  - 3.7 ISAE 3402 ..... 10
  - 3.8 ISF STANDARD OF GOOD PRACTICE for Information Security and INFORMATION SECURITY FOR EXTERNAL SUPPLIERS ..... 10
  - 3.9 COMMON ASSURANCE MATURITY MODEL (CMM)..... 10
- 4 THE FUTURE.....11**
  - 4.1 NEED FOR A GLOBAL REPOSITORY..... 11
  - 4.2 A MODULAR APPROACH .....12
- 5 CONCLUSIONS ..... 13**
  - 5.1 PROJECTED TIMELINE.....13
  - 5.2 PROPOSED WORKING FORMAT .....13

# 1 INTRODUCTION

## 1.1 PURPOSE

This paper has been written to provide the reader with an overview of the assurance landscape. In particular it is intended to define the issues with the multitude of assurance frameworks currently available and in certain cases mandatory. With the changing business environment, and budgetary constraints affecting there is a clear need for organizations to maximize value in providing assurance. This paper defines the combined vision of leading professional and industry bodies providing assurance frameworks to provide greater efficiencies for all organizations regardless of geography, industry or size.

## 1.2 AUDIENCE

Business leaders, executives and managers

IT and Information security leaders, managers, professionals and professional bodies

Buyers / acquirers of services

Service providers (including IT and cloud service providers)

Auditors

## 1.3 APPROACH

This paper is the result of a global collaboration between private organizations, professional bodies and experts. Each has contributed insights, experiences, suggestions for controls and time (for free) to create a shared vision for business assurance. This shared vision has been edited, reviewed and organized by the authors representing these professional bodies to produce the collaborative, coordinated vision for businesses in the 21<sup>st</sup> century.

## 2 CURRENT APPROACHES TO ASSURANCE

### 2.1 A COMPLICATED ENVIRONMENT

Modern organizations sit in a complex web of customers and external suppliers that can span the globe. From an information perspective, the standards that organizations can adopt to protect their information are constantly evolving to satisfy changing business models, regulatory and other requirements. One of the challenges facing organizations are the multitude of assurance frameworks, which in many cases result in duplication and ultimately inefficiencies, but also may leave gaps resulting in greater risk to organizations.

Since technology plays a key role in this dynamic business environment characterized by high numbers of short-term relationships, the increasing reliance on third parties to handle one's information, if not effectively managed, can represent a significant risk to organizations. This ultimately means that organizations are forced to gain assurance from more third parties while lacking the tools to do so with an efficient and scalable approach. Added to this is the complexity of multiple professional, regulatory and expert bodies that have created a number of disparate standards to help protect and secure information. Current assurance models typically operate in isolation and are predominantly focused internally on protecting an organization and its information, and do not easily extend to its partners, suppliers, and customers. Organisations are thus faced with three issues:

1. Difficulty in defining generally accepted standards for protecting information in the increasingly dynamic business environment
2. Lack of a common standard to apply across the value chain / business cycle
3. Incompatible assurance frameworks, and the inability to share translate existing assurance practices by third parties.

### 2.2 A GLOBAL PERSPECTIVE

First there was the integrated organization with a self contained value chain, whereby a single organisation would carry out the primary and secondary activities needed to deliver goods and / or services to its customers. Today we have 'unbundling', 'disintermediation' and focus on core competences, which mean that organizations no longer conduct all the activities to deliver goods and services – they now rely on a complex web of multiple external partners – not just for inputs – but for logistics, service and support activities.

To make this complex web of organizations work, information has to be shared across multiple organizations and in multiple ways. This information may contain trade secrets, intellectual property and / or personal information and it needs to be protected according to business impact as well as satisfying regulatory and legal requirements. The acquiring organization needs to understand the information security arrangements of both potential and actual partners and be able to answer several questions, including:

- What level of protection are the partners capable of applying to my information (including information I have been trusted with by my customers)?
- How do their practices compare my arrangements?
- How well do they comply with relevant regulation and legislation?
- How do potential partners practices compare against each other?

Gaining assurance in this landscape is often the responsibility of the end customer assuring themselves that the primary contractor, and in many cases the subcontractors do not represent an unacceptable risk to the business. Subsequently the cost is borne by the end customer, equally the primary contractor is often faced with multiple end customers demanding assurance in differing ways. However, with the results of assurance activities not being shared between end customers the primary contractor is faced with multiple duplicating activities consuming considerable resources.

This paper presents an approach to communicating assurance among transacting and partnering organizations that helps to address many of the issues outlined above.

## 3 KEY STAKEHOLDERS

The following details the key stakeholders that define the need or Standards for effecting control or gaining assurance.

### 3.1 PCI-DSS

Name: Data Security Standard (now at version 2)

Organisation: Payment Card Industry Security Standards Council

Scope: The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data.

Website: [https://www.pcisecuritystandards.org/security\\_standards/index.php](https://www.pcisecuritystandards.org/security_standards/index.php)

### 3.2 CLOUD SECURITY ALLIANCE

Name: Cloud Controls Matrix

Organisation: Cloud Security Alliance

Scope: The Cloud Security Alliance Cloud Controls Matrix (CCM) is specifically designed to provide fundamental security principles to guide cloud service providers and to assist prospective cloud customers in assessing the overall security risk of a cloud provider. The CSA CCM provides a controls framework that provides a detailed understanding of security concepts and principles that are aligned to the Cloud Security Alliance guidance in 13 domains.

The foundations of the Cloud Security Alliance Controls Matrix rest on its customized relationship to other industry-accepted security standards, regulations, and controls frameworks such as the ISO 27001/27002, ISACA COBIT, ISF, PCI, and NIST, and will augment or provide internal control direction for SAS 70 attestations provided by cloud providers. As a framework, the CSA CCM provides organizations with the needed structure, detail and clarity relating to information security tailored to the cloud industry. The CSA CCM strengthens existing information security control environments by emphasizing business information security control requirements, reduces and identifies consistent security threats and vulnerabilities in the cloud, provides standardize security and operational risk management, and seeks to normalize security expectations, cloud taxonomy and terminology, and security measures implemented in the cloud.

Website: <https://cloudsecurityalliance.org/>

### 3.3 SP800

Name: Special Publication series

Organisation: National Institute of Standards and Technology

Scope: Special Publications in the 800 series present documents of general interest to the computer security community. The Special Publication 800 series was established in 1990 to provide a separate identity for information technology security publications. This Special Publication 800 series reports on ITL's research, guidelines, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations.

Website: <http://csrc.nist.gov/>

### 3.4 ISO / IEC 27xxx

#### 3.4.1 ISO / IEC 27001/2

Name: ISO/IEC 27001:2005 Information technology -- Security techniques -- Information security management systems – Requirements

ISO/IEC 27002:2005 Information technology -- Security techniques -- Code of practice for information security management

Organisation: International Standards Organisation

Scope: ISO/IEC 27001:2005 covers all types of organizations (e.g. commercial enterprises, government agencies, not-for profit organizations). ISO/IEC 27001:2005 specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System within the context of the organization's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof.

ISO/IEC 27001:2005 is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties.

ISO/IEC 27002:2005 comprises ISO/IEC 17799:2005 and ISO/IEC 17799:2005/Cor.1:2007. Its technical content is identical to that of ISO/IEC 17799:2005. ISO/IEC 17799:2005/Cor.1:2007 changes the reference number of the standard from 17799 to 27002.

ISO/IEC 27002:2005 establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined provide general guidance on the commonly accepted goals of information security management. ISO/IEC 27002:2005 contains best practices of control objectives and controls in the following areas of information security management:

- 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;
- Information security incident management;
- Business continuity management;
- Compliance.

Website: [http://www.iso.org/iso/catalogue\\_detail?csnumber=42103](http://www.iso.org/iso/catalogue_detail?csnumber=42103) and [http://www.iso.org/iso/catalogue\\_detail?csnumber=50297](http://www.iso.org/iso/catalogue_detail?csnumber=50297)

### **3.4.2 ISO / IEC 27036**

Name: ISO/IEC NP 27036 (<http://www.iso.org/iso/rss.xml?csnumber=44380&rss=detail>)  
Information technology -- Security techniques -- Information security for supplier relationships (DRAFT)

Organisation: International Standards Organisation

Scope: multi-part standard Part 1 – overall, Part 2 - , Part 3 - , Part 4 - ,

ISO/IEC 27036 will be a multi-part standard offering guidance on the evaluation and mitigation of security risks involved in the procurement and use of information or IT-related services supplied by other organizations. It is planned to cover the following broad areas:

- Strategic goals, objectives and business needs in relation to information security;
- Information security risks and mitigation techniques;
- Provision of assurance (and presumably compliance with contractual obligations etc.).

ISO/IEC 27036-1 - Overview and concepts

An initial working draft of Part 1 has been released to SC27. The working title is “Information technology – Security techniques – Information security for supplier relationships – Part 1: Overview and concepts”.

ISO/IEC 27036-2 - Common requirements Section added March 9

A preliminary working draft of Part 2 has been released to SC27. The working title is “Information technology – Security techniques – Information security for supplier relationships – Part 2:

Common requirements”. As currently drafted, the main text appears to be laying out formal requirements, with advisory ‘implementation guidance’ in an annex.

Website:

[http://www.iso.org/iso/iso\\_catalogue/catalogue\\_tc/catalogue\\_detail.htm?csnumber=44380&commid=45020](http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=44380&commid=45020)

### 3.5 SHARED ASSESSMENTS PROGRAM

Name: Standardized Information Gathering (SIG) questionnaire version 6.2, AUP version 5.0

Organisation: Financial Services Roundtable

Scope: The Shared Assessments Program offers a common-sense approach to evaluating vendor controls for security, privacy and business continuity. By using the Shared Assessments tools, outsourcers, service providers and assessment firms save time, resources and money by reducing redundancies and increasing efficiencies in the vendor control assessment process.

With the Standardized Information Gathering Questionnaire (the SIG), service providers complete one questionnaire and provide it to multiple clients. Outsourcers get faster turnaround from their service providers - in some cases receiving a detailed questionnaire the same day that they request it.

For higher-risk relationships or services, the Agreed Upon Procedures (the AUPs), may be used to objectively test key controls in the service providers environment and create a detailed report of the results. As with the SIG questionnaire, service providers may provide an AUP report to an unlimited number of clients. In some cases, the AUP report executed by an independent accounting or assessment firm can reduce or even eliminate the need for costly on-site assessments.

The Shared Assessments AUP and SIG were developed by Shared Assessments Program members and are updated at least once annually.

Website: <http://www.sharedassessments.org/>

### 3.6 COBIT

Name: Common Objectives for Information and related Technology (now version 4.1)

Organisation: ISACA

Scope: COBIT is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks. COBIT enables clear policy development and good practice for IT control throughout organizations. COBIT emphasizes regulatory compliance, helps organizations to increase the value attained from IT, enables alignment and simplifies implementation of the COBIT framework.

Website: <http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx>

### 3.7 ISAE 3402

Name: International Standard on Assurance Engagements (ISAE) 3402 Assurance Reports on Controls at a Service Organisation

Organisation: International Federation of Accountants

Scope: This International Standard on Assurance Engagements (ISAE) deals with assurance engagements undertaken by a professional accountant in public practice to provide a report for use by user entities and their auditors on the controls at a service organization that provides a service to user entities that is likely to be relevant to user entities' internal control as it relates to financial reporting.

Website: <http://web.ifac.org/download/b014-2010-iaasb-handbook-isa-3402.pdf>

### 3.8 ISF STANDARD OF GOOD PRACTICE for Information Security and INFORMATION SECURITY FOR EXTERNAL SUPPLIERS

Name: Information security standard and explicit requirements for external suppliers

Organisation: Information Security Forum

Scope: The Standard of Good Practice for Information Security is the most practical source of information security and information risk related guidance available world-wide. Significantly updated each year, the standard addresses information security from a business perspective and provides a basis for assessing and improving an organization's information security arrangements.

The Information security for external suppliers baseline report provides information security professionals with a set of common security arrangements that can be applied to all external suppliers, based on a combination of real-world experience, good practice and ISF research and analysis.

For more information: <https://www.securityforum.org>

### 3.9 COMMON ASSURANCE MATURITY MODEL (CMM)

Name: Common Assurance Maturity Model

Scope: A global collaborative project that aims to provide a framework to support transparency in attesting the Information Assurance Maturity of Third Party Providers & Suppliers (e.g. Cloud providers). It aims to publish results in an open and transparent manner, without the mandatory need for third party audit functions, or due diligence engagements. This approach allows data processors to demonstratively publicise their attention to Information Assurance in comparison to other supplier's levels of compliance, and security profiles. Subsequently negating the operational requirement for time consuming, expensive, subjective, and resource intensive bespoke arrangements to attest security and compliance.

Website: <http://www.common-assurance.com>

## 4 THE FUTURE

### 4.1 NEED FOR A GLOBAL REPOSITORY

Without any tangible collaboration and consistency between the various assurance frameworks organizations are forced to develop and implement a subjective body of knowledge that best articulates their risk appetite. Such activities are invariably resource intensive, both in terms of development, but equally the supplier is potentially required to provide individual responses for each customer.

There exists a business need to develop a mechanism that allows suppliers to respond once, and share with many. Such a development will provide significant efficiencies for the supplier, in that a single (or a small number of) assessments can be used by multiple customers. Equally, this would enable customers to quickly assess the large number of third parties in their supply chain without individually assessing each third party provider.

An additional advantage of such an approach is that it would provide transparency in the assurance of the supply chain. In particular, suppliers could understand the detailed requirements placed upon them before entering a contractual agreement with customers.

Any such mechanism would allow contributing organizations to:

1. Self-assess their security; OR
2. Be assessed by an independent organization

The results of assessments could be:

1. Published by suppliers on their website
2. Submitted to independent 'trusted' authorities for certification / confirmation
3. Held by an independent authority for potential customers to examine
4. Published and made available globally to buyers, suppliers, auditors etc.

Moreover such a repository could allow organizations to advertise their services, and level of Information Assurance maturity to potential customers. Such an approach would make it easier for organizations to select suppliers and partners based on the maturity of their information assurance practices.

The authors of this paper and organizations they represent fully support the need for a global approach and repository. Moreover, it is agreed that such an initiative and repository should be independent and 'not for profit' in order to ensure its focus, provide transparency and secure wider endorsement.

### 4.2 A MODULAR APPROACH

The global repository, or ‘Third Party Assurance Centre’ will support in the first instance a select number of assurance frameworks. Support would be enabled in a modular fashion, whereby a user could select the appropriate modules based on business requirements, as depicted in Figure 1.

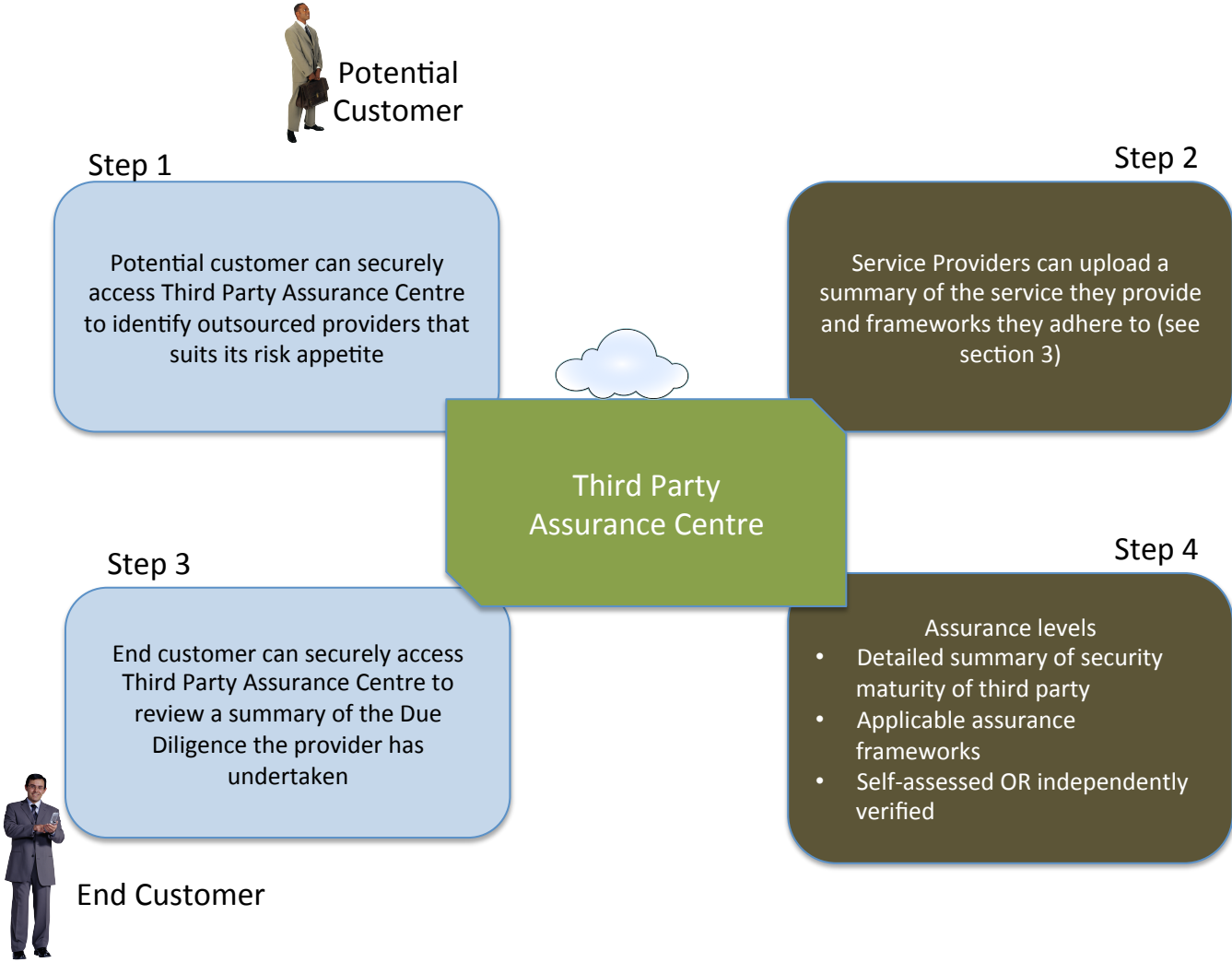


FIGURE 1: MODULAR APPROACH

## 5 CONCLUSIONS

### 5.1 PROJECTED TIMELINE

This document represents the shared vision between the professional associations. It will be followed up by a more detailed working document that will encompass the governance for the proposed mechanisms and Third Party Assurance Centre.

### 5.2 PROPOSED WORKING FORMAT

Representatives from the author organizations will work collaboratively to outline and publish the detailed governance document. Prior to any release the document(s) will undergo review within the respective organizations.