

Common Assurance Maturity Model Guiding Principles

Issue: 1st November 2010

About this Document

This document summarizes the fundamental principles of the Common Assurance Maturity Model (CAMM), and related activities including the Third Party Assurance Centre (TPAC).

It is intended to provide the reader an overview of CAMM, its anticipated modus operandi, and the benefits it can provide to business as well as a roadmap of the overall project.

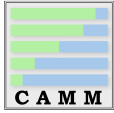
This document will be followed by a more detailed paper that will provide further detail on the key points presented within this paper.

Audience

This document represents the consensus of the CAMM steering committee on the guiding principles and direction for the CAMM project. It should be read by those persons interested in gaining a greater understanding on the CAMM project.

Context

This document provides a summary of CAMM, and associated activities. Additional detail on the project will be captured in a subsequent, more detailed paper and www.common-assurance.com.



Common Assurance Maturity Model

“The new business assurance barometer.”

Key Benefits

The Common Assurance Maturity Model (CAMM) is designed to provide trustworthiness (safety, security and reliability) of the supply chain working within and across the Internet in the new information world. It offers the following benefits to customer and service provider organizations:

Mission Statement

Provide an **objective, consistent and complete** trust framework to **transparently** assure **information risk management maturity** across the **supply chain**.

Provide objective assessments to compare options and influence purchasing decisions: CAMM allows customers to compare the information risk management maturity of different service implementation alternatives, including in-house implementation choices as well as ones involving components outsourced to external providers.

Reduction in compliance cost and effort: CAMM allows service providers to derive more benefit from fewer compliance exercises whose summary results can be shared amongst customers, with the control of how much information to be divulged remaining with the provider. Customers can undertake assessments without having to understand the complexities of technical controls, or undertaking numerous site audits.

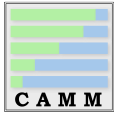
Increased business agility: CAMM allows customers to more rapidly screen and engage service providers to gain assurance that their information will be managed within their risk appetite. Long protracted assessments can now be conducted within hours and can unlock the potential of the cloud to provide resources on short-notice contracts.

Leverage existing compliance expenditure: CAMM is derived from current industry standards, with domains created by subject-matter experts in the respective domains. All CAMM controls that are derived from an existing framework have clear lineage to ensure that money and resources already spent on assessments are not wasted.

Clear strategic direction on how to attain higher levels of maturity: All CAMM controls are structured and assessed using criteria which provide a clear path of where to improve in the event that a service provider wishes to gain higher levels of maturity to gain more business.

Engagement with all sizes of organizations: CAMM has been created with all sizes of services, providers, and customers in mind. Service profiles ensure that organizations of different sizes can be assessed in a similar fashion. Customers make the choice of supplier based on the level of maturity in the domains they require as a result of assessing themselves. Service providers can attain the lower levels of maturity to engage with CAMM and can continue relying on it as their service matures. Language within the controls is also designed to be accessible to all levels of experience.

Emphasis on risk management: CAMM is not designed to be a framework where the lowest common denominator, or indeed technical excellence in controls, is the focus, but one where service providers can show how well they manage the design and implementation of controls in relation to the confidentiality, integrity and/or availability of information.



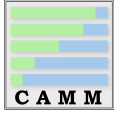
Common Assurance Maturity Model

“The new business assurance barometer.”

Problem Statement

CAMM is a response to the following problems:

- **Organizations are under pressure to reduce costs:** Organizations are increasingly being asked to do more with less, outsourced IT services such as cloud computing offer cost savings which are very hard for most businesses and governments to ignore in the current economic climate. Even if they are not outsourcing, consolidation of data centers or IT functions within large organizations is becoming more common. It is difficult to justify maintaining in-house IT provision at a business unit level when the same service can be consolidated/outsourced for a tenth of the price, often with better service performance and, potentially, with better management of information risks.
- **Lack of transparent communication of security policies and process:** Both services providers and their clients are lacking a standard means to evaluate offers on the basis of their security, even though security is seen as a prime concern by most organizations. As a result, either customers cannot compare offerings on security, or service providers are duplicating the effort of providing information many times over. This is not only wasteful but also reduces the overall security of the organization since instead of auditing just once; many more third parties must be given access to infrastructure.
- **Challenges in evaluating trustworthiness (safety, security and reliability – manifested through information risk management maturity) across the service supply chain:** Current assurance and risk management frameworks are designed for a world in which each organization’s IT services are self-contained, but the reality is that IT services are delivered through a supply chain involving many components and organizations (for instance cloud computing services, outsourced IT management, etc.) that provide varying degrees of transparency and control in managing associated risk. The old adage that ‘security is only as strong as the weakest link’ is ever more relevant, but faced with this bewildering set of interdependencies, many organizations ask themselves “where should we stop”. A common trust framework is required.
- **Focus on technical excellence rather than management of risks:** Despite the myriad of frameworks to manage information risks, information breaches are still common place, even in accredited systems. Data controls are being implemented at the technical level, with scant regard for the engagement of the business owners in understanding the context of the information being managed.



Common Assurance Maturity Model

“The new business assurance barometer.”

The CAMM solution

The Common Assurance Maturity Model (CAMM) has been created by a consortium of end user organizations, service providers, associations, and government bodies with the aim of providing transparency on information risk management maturity, *across the IT services supply chain*. Ultimately, this transparency will make it easier for customers to pick solutions that best meet their specific risk appetites.

CAMM provides a set of core controls based on existing standards that are seen as absolutely essential to ALL solutions irrespective of size, geography, or industry.

Such core controls allow the efficient assessment of key risks to an organization. Completion of the assessment provides an output maturity score for the specific domain areas for a given service profile. This score represents the information risk management maturity (and thus trustworthiness in information transactions) of the service based on the core controls.

These core controls can then be supplemented by additional modules (e.g. an EU data protection module, financial services, or a PCI-DSS module) that can either be provided by the CAMM team or by the wider information security community. This **modular approach** allows organizations to identify the areas important to their business.

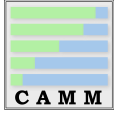
The CAMM framework is underpinned by the following key principles;

Transparency and trustworthiness

Completion of the CAMM assessment must provide business and governments with full visibility of risks. CAMM achieves transparency as follows:

- **Common language:** CAMM defines key terms and controls according to commonly understood industry frameworks to manage risks to information. Services that are assessed by CAMM will be required to complete a service profile which will be available with the assessment to provide weighting and context to the responses provided.
- **Objective criteria:** CAMM provides a combination of quantitative and qualitative controls which leverage an assessment of the IT service to provide objective criteria by which the information risk management maturity of different service providers can be compared to influence a purchasing decision.
- **Impact-focused scoring criteria:** CAMM is designed to leverage the design and implementation maturity of controls to create measurements at a control, control objective and domain level. This ensures that where governance impacts the performance of qualitative controls, that this impact is taken into account.

A **modular approach** allows organizations to identify the areas important to their business.



Common Assurance Maturity Model

“The new business assurance barometer.”

- **Trusted Auditors:** CAMM’s controls and guidance will be accompanied by a trusted third party auditor scheme. All auditors will be accredited by a third party non-profit accreditation scheme which will guarantee its veracity and independence.

Complementary and compatibility

CAMM is based on existing frameworks including ISO/IEC-27001:2005, PCI-DSS, COBIT, ENISA EAF and the CSA Controls Matrix. This means that organizations already implementing these frameworks will be able to leverage existing investment.

Completeness

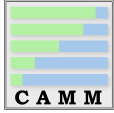
It’s accepted that security is only as strong as the weakest link, and the management of information risks is no exception. Therefore CAMM must be able to assess all relevant components and architectural layers of a complete end-to-end service.

The potential of a combined CAMM assessment of the elements that comprise an end-to-end service offering, allows organizations to understand the **total risk** of the service. Based on this, the organization can determine whether the risk is acceptable and if not, which elements they need to focus on to achieve the desired risk profile.

Accessibility

CAMM provides a common language that is accessible, at different levels of understanding, to all stakeholders regardless of their technical knowledge and capability. The net result of the process means that the appropriate level of detail is provided to key stakeholders, making the framework accessible to all.

1. Senior Management are provided the aggregated score, and can also quantify the level of assessment required to achieve greater confidence.
2. Periodically, security professionals receive more detailed assessments of IA maturity within third parties. Note: Potentially, this may also include independent verification from third parties; however the use of CAMM does not necessitate a subscription.
3. Third parties: Are provided specific details from customers, and business partners detailing the exact requirements demanded.



Common Assurance Maturity Model

“The new business assurance barometer.”

Efficiency

CAMM provides a means of easily communicating information risk management maturity between parties looking to enter into a service relationship. This avoids the need for bespoke requirement review, reduces audit process cost and lessens time to market for the service suppliers and customers.

1. External third party service providers will be able to complete and publish one set of assurance activities that will be able to satisfy the vast majority of customers, rather than undertaking individual bespoke activities.
2. CAMM will identify the need for third parties to meet key security requirements before initiating a relationship. This is also of benefit to third parties who will know exactly what is required before any investment is made.

Tools are to be developed to enable the CAMM score to be easily derived from responses to standardized questions and the values of objective metrics. This reduces the need for bespoke audit and contractual arrangements. Furthermore, the tools will allow CAMM scores to be combined for different components of an end-to-end service into a composite service CAMM score, if required.

Modularity and extensibility

Assurance requirements for many organizations change depending on many factors including geography, industry, and/or risk appetite. CAMM adopts a modular approach to provide flexibility and adaptability. The framework will allow for defining controls modules to benchmark against specific regulatory (e.g. HIPAA, PCI DSS, etc.), vertical and lateral (e.g. CNI, business continuity, etc.) or technological (e.g. SaaS, IaaS, PaaS) requirements.

Relevance

The application of the framework will help organizations to evaluate the relevant assurance levels and compare these among alternative service implementations to inform risk decisions. This is ensured via a collaborative approach between the key industry organizations, regulators and standardization bodies.

Consistency

CAMM provides consistency in the semantics of different levels of abstraction through weighting and mapping schemes making it easy to compare results from different solutions, components, and service providers. CAMM provides a consistency between:

1. Service profiles being present for each assessment
2. Scoring of controls using the design and implementation of the control to derive a score
3. Consistency in auditor accreditation criteria.