the information security provider

A Framework for IT Security Assurance:

Do You Understand How All of Your IT Security Assurance Efforts Fit Together?

Fiona Pattinson

Austin ISSA: 19th January, 2012

Email: fiona@atsec.com

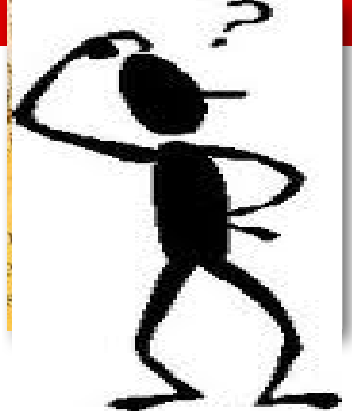
Key Takeaways

1) An understanding of the key terminology and concepts of IT security assurance.

2) An understanding of the various types of methods for providing security assurance.

3) An understanding of aspects of security assurance methods to determine the strengths and weaknesses of each.

What Do They Mean To You?



Certificate No. IS 563070

QUALIFIED SECURITY ASSESSOR

cve.mitre.org

FIPS 140-2

Security Configuration CHECKLISTS http://checklists.nist.gov CSD

SANS

Drummond certified COMPLETE EHR INPATIENT

CISCO CERTIFIED CCNA SECURITY

CC EAL 7+ THE HIGHEST EVALUATED PRODUCT IN THE WORLD

SAS 70 Type II

FedRAMP

CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL CISSP

CERTIFIED PENETRATION IACRB TESTER

NASPO CERTIFIED SECURE

C-level Security CERTIFIED

CISM CERTIFIED INFORMATION SECURITY MANAGER

Diacap

TIER-3 DATA CENTERS SAS-70 TYPE II CERTIFIED

SOGIS IT SECURITY CERTIFIED

ISO 27001 CERTIFIED

FIPS 140-2 CRYPTOGRAPHY

Microsoft Security Essentials

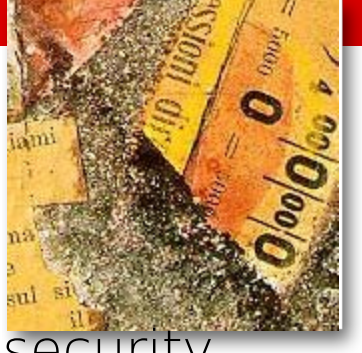
SANS TOP 20 LIST THE TWENTY MOST CRITICAL INTERNET SECURITY VULNERABILITIES

CERTIFIED ISO 27001

CCEVS Validation Body

CompTIA Security+ CERTIFIED

Common Criteria



- These (and other) marks indicate a claim about the security "goodness" of the organization, product, service, or person that they are associated with.
- Often associated with some kind of conformity assessment with the aim of providing "security assurance" to those relying on them.
- But the "goodness" can be very variable and depends on:
  - The needs of the person depending on the claims
  - The confidence that the person depending on the claims can place in how.

Definitions of "Assurance"

as·sur·ance *noun* \ə-'shůr-ən(t)s\

Merriam-Webster

Definition of ASSURANCE

1 : the act or action of assuring: as

a : PLEDGE, GUARANTEE

b : the act of conveying real property; *also* : the instrument by which it is conveyed

c *chiefly British* : INSURANCE

2 : the state of being assured: as

a : SECURITY

b : a being certain in the mind <the puritan's *assurance* of salvation>

c : confidence of mind or manner : easy freedom from self-doubt or uncertainty; *also* : excessive self-confidence : BRASHNESS, PRESUMPTION

3 : something that inspires or tends to inspire confidence <gave repeated *assurances* of goodwill>

ISO

"grounds for justified confidence that a claim has been or will be achieved"

(ISO/IEC TR 15026-1:2010)

Security is Related to Quality

- Security assurance is related to quality assurance.
- Quality has been defined in many ways including:
  - excellence or arête (Socrates, Plato, Aristotle);
  - value (Feigenbaum);
  - conformance to specification (Gilmore, Levitt, Crosby, Deming, Feigenbaum, Juran);
  - meeting/exceeding customers expectations (Feigenbaum, Juran);
  - conformance to requirements (Crosby);
  - loss avoidance (Taguchi);
  - fitness for purpose (Juran).

Different philosophies… When it comes to IT security assurance which are yours, which are your customer's ?

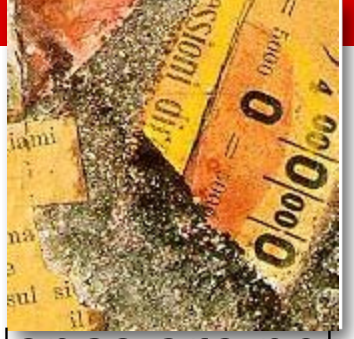
True or False?

- Providing IT security assurance will":
  - A) be resource intensive ? **Yes**
  - B) add costs to the process ? **Yes**
  - C) add delays to the process ? **Yes**

Is it a fair criticism of security assurance schemes that these properties are true?

- Providing good security assurance can:
  - A) confirm a claim that something is "completely secure" ? **No**
  - B) add safeguards or services to the deliverable? **No**
  - C) add strength to assurance mechanisms? **No: You can't test quality into a product either!**
  - D) ensure that the security objectives are the correct objectives? **No: You assurance can show that the objectives are met, but not that the right objectives were specified in the first place.**
  - E) reduce risk? **Yes**
  - F) improve the product? **No**

Assurance ≠ Confidence

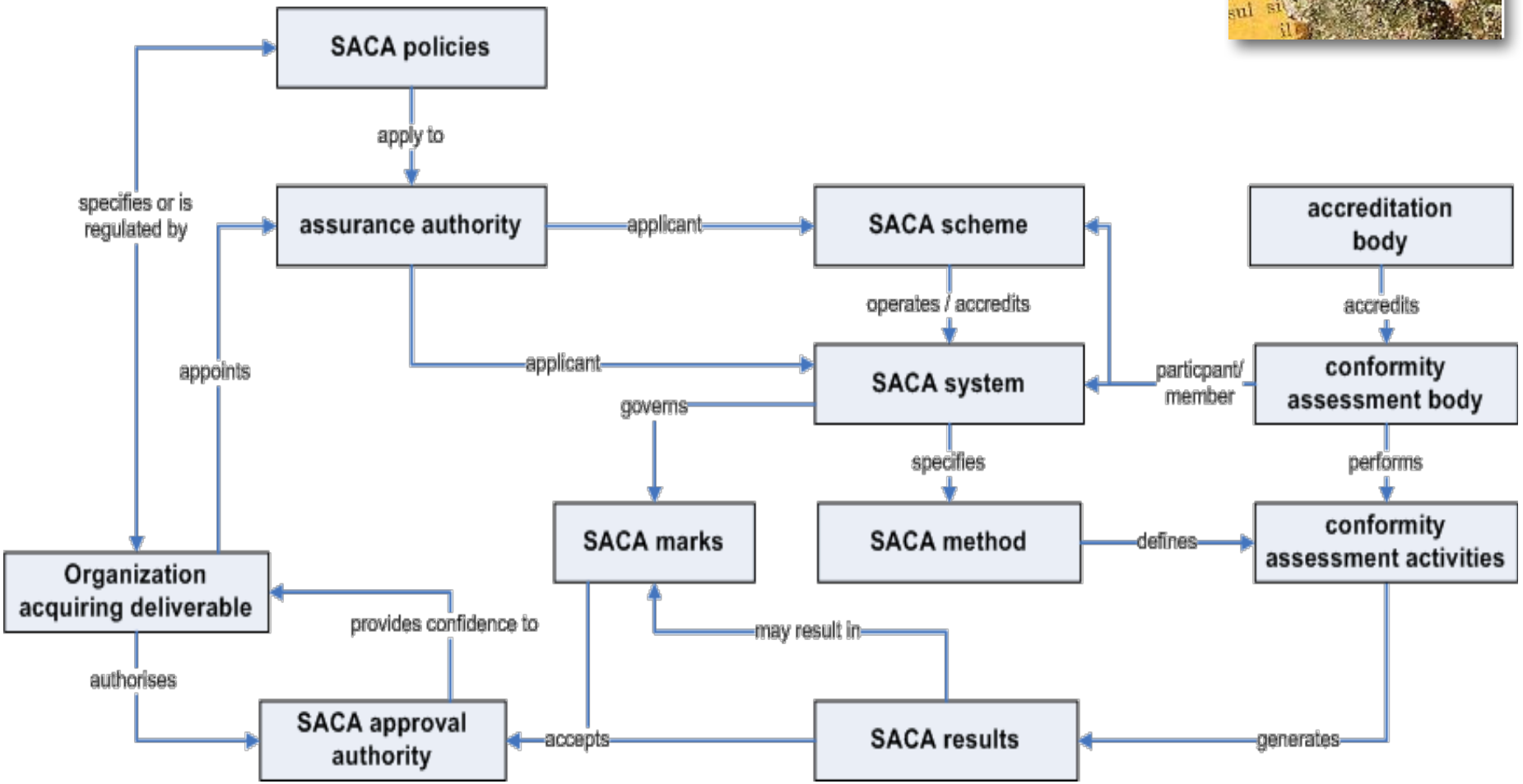


- It is important to point out that assurance and confidence are not identical and cannot be used in place of one another.
  - Confidence is related to the belief that one has in the assurance of the deliverable and may vary from person to person because of different knowledge and understanding of.
    - the assurance criteria used
    - the method used
    - the assurance scheme
  - Assurance is related to the demonstrated ability of the deliverable to perform its security objectives.

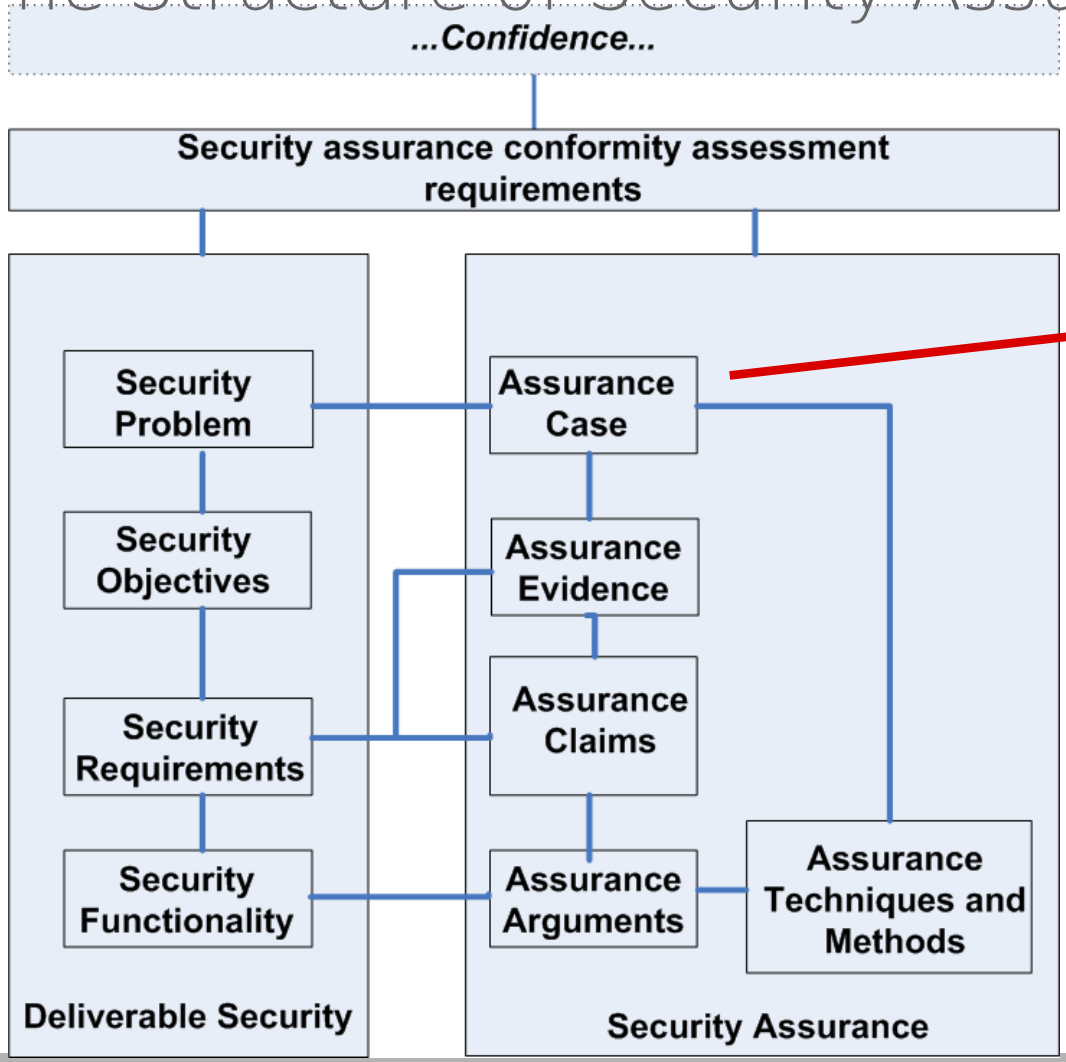
Stakeholders

- security assurance is sought by those having assets at risk through the operation of deliverable. E.g.
  - governments, who can require security assurance through legislation and regulations;
  - specific communities who have assets, including their reputation, at risk and who can regulate or define best practices for that community (e.g. the payment card industry);
  - organizations who are responsible for protecting their own assets, or who operate IT systems protecting the assets of other third parties;
  - integrators and suppliers of IT systems to acquirers;
  - end users, who have a security problem to address and who may be able to influence the specification of security requirements either directly, or indirectly; and
  - developers and suppliers of the deliverables that form the components of an IT system.

Relationships in Security Assurance Conformity Assessment

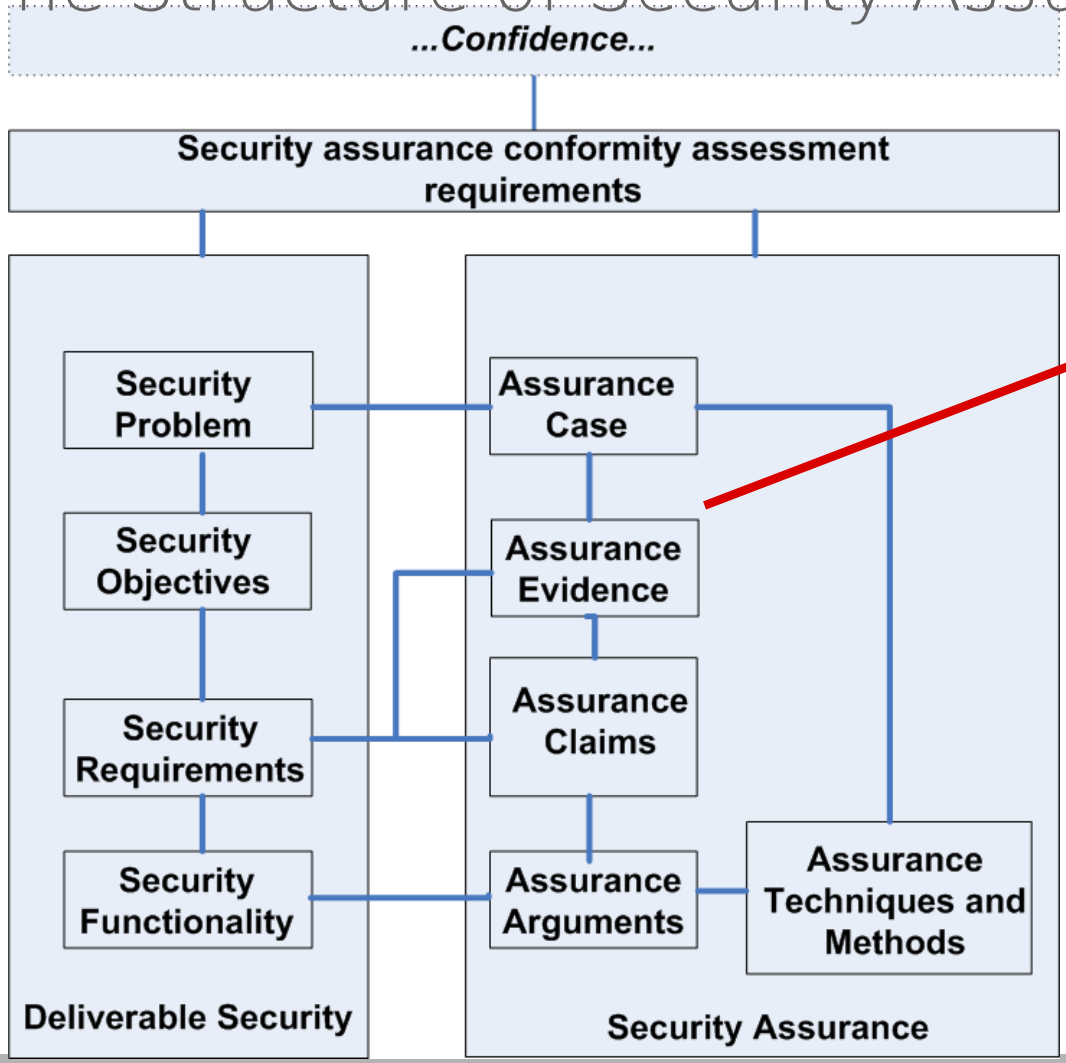


The Structure of Security Assurance



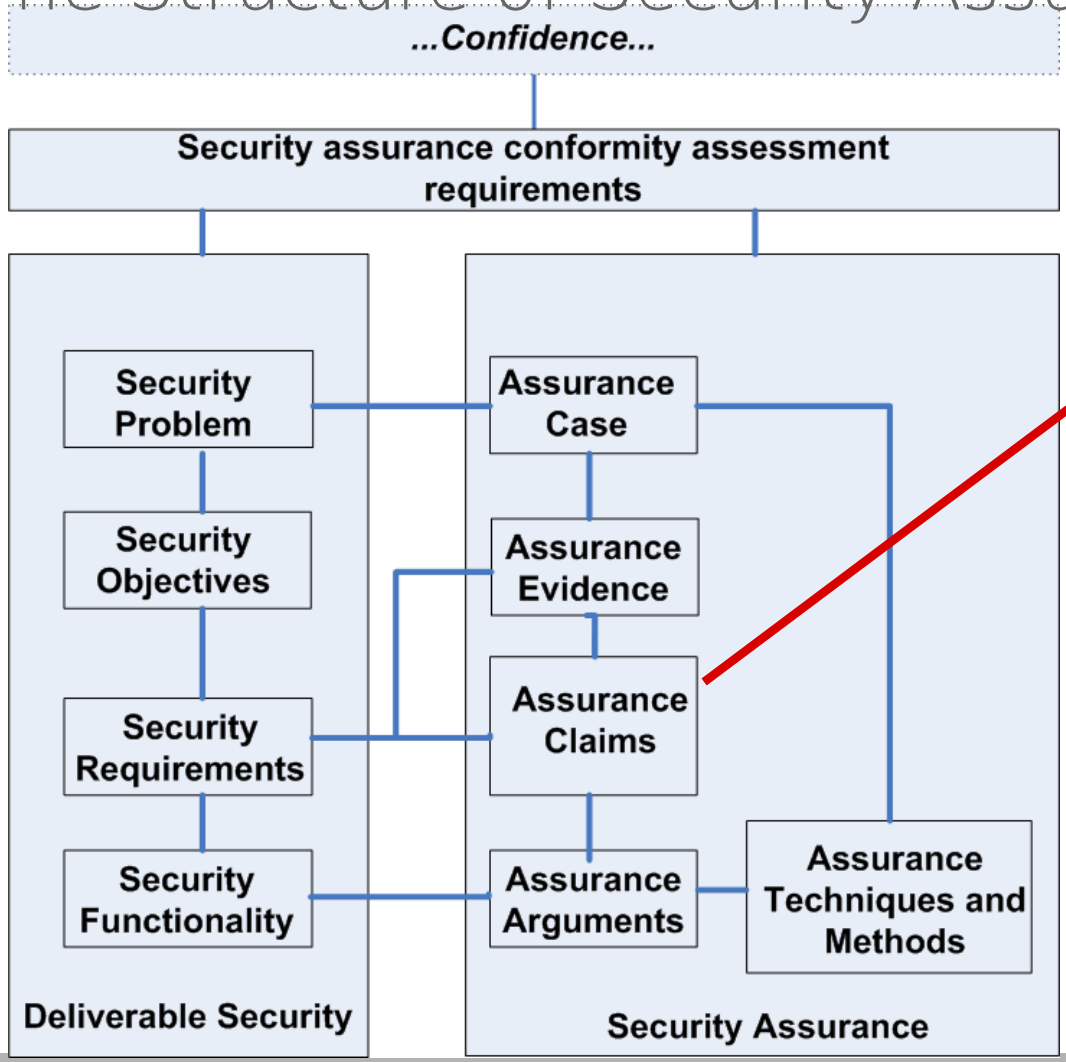
A security assurance case is an overall package of security assurance related to the IT system. It demonstrates how, and with what confidence, the security assurance requirements for an IT system have been met. The security assurance case may be represented in a variety of ways and forms. The security assurance case provides the confidence and trust that the user of the IT system may have in the security of the IT system

The Structure of Security Assurance



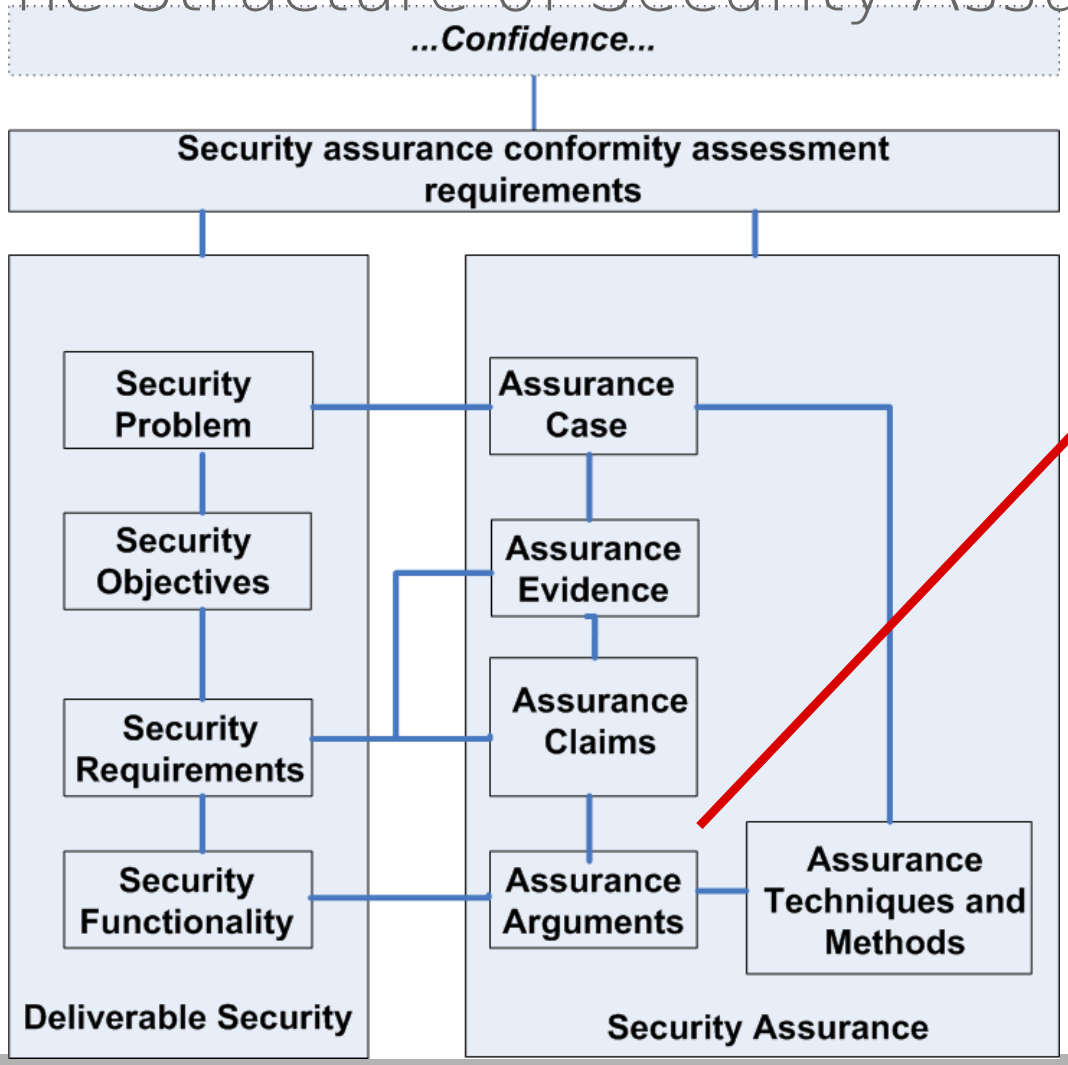
There are many forms of security assurance evidence that can be presented to support a security assurance case. However, what is important about the evidence is that it is demonstrable, repeatable, and defendable.

The Structure of Security Assurance



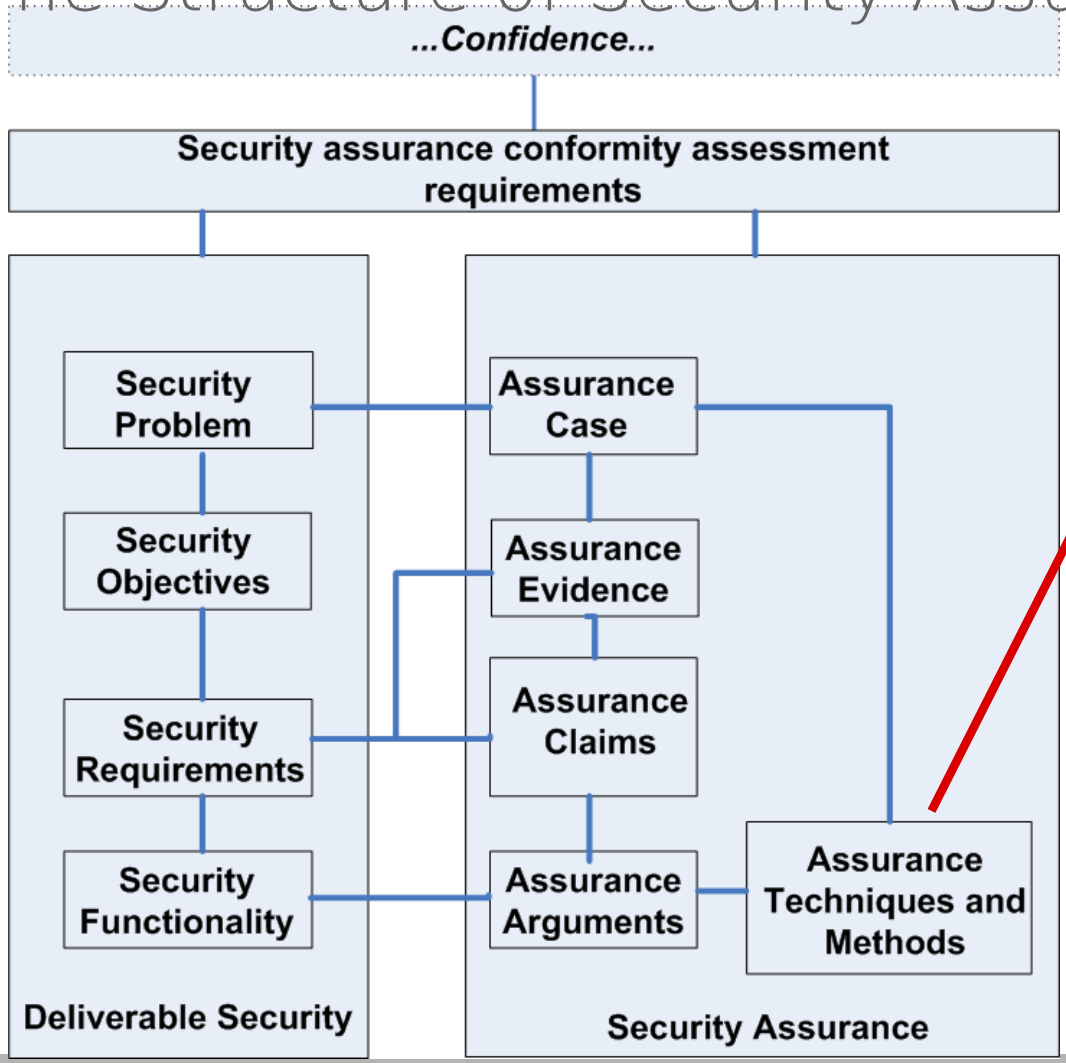
Security assurance claims come in many different types and can also be used in many different ways. They are often for different purposes.
Assurance claims are often represented as "Marks or Symbols" that may be applied to the product or service. Marks and symbols come in many types ranging from registered and certified marks that include "Third Party" testing and certification of the product or service, to symbols that include the registered Logo of the product or sub-assembly.
Symbols are often used for "authenticating" the origin of the product or service.

The Structure of Security Assurance



Assurance arguments are based on:
- testing and evaluation of the product or service;
- the reputation of the supplier;
- the professional competence of the engineers performing the work; and
- the maturity of the processes used.
- the methods used in the design of the product or service;
- the tools used in the design of the product;
- the tools used in the performance of the service.

The Structure of Security Assurance



Typically, the technical requirements for providing SACA results are presented separately to the method for testing that the requirements are met. This allows for the possibility of different SACA methods to be applied to a particular set of requirements, but means that understanding the method applied is an important part of understanding the assurance given.

Methods

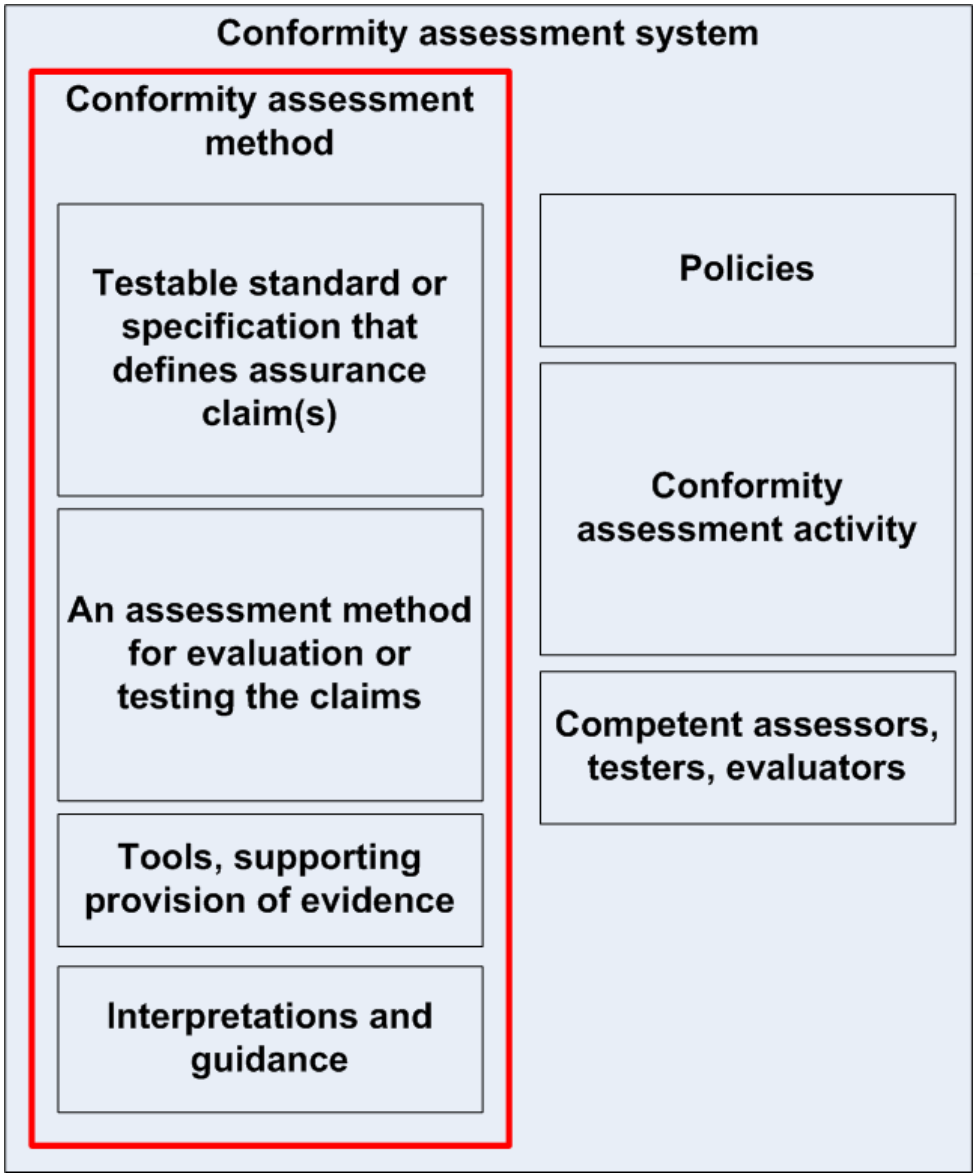
Methods may employ different techniques:

- **Direct Assessment**
- **Indirect Assessment**

(Look at the deliverable, or the processes and components that make the deliverable)

- **Static Assessment**
- **Dynamic Assessment**

(Look at the deliverable, before operation or in a lab or in the operational state)



Techniques for security assurance conformance assessment (SACA)

Effectiveness (or evaluation)

This technique allows for the security assurance claim to be tailored in order to meet the deliverable at hand or the specific requirements of the stakeholder specifying the assurance requirements.

It provides a very flexible way of providing an security assurance claim or claims, but requires great care by the consumer of the security assurance claim to fully understand the actual assurance provided.

Typically the assurance claims made by one instance of applying the method may not be directly comparable to another instance

Examples: Common Criteria; ISO/IEC 27001

Techniques for security assurance conformance assessment (SACA)

Correctness (or conformance)

A correctness technique supports an assurance claim based on conformance to a standardised specification. Typically there is little flexibility in what is evaluated or how.

The deliverable either meets the specified requirements or it does not.

Examples: FIPS 140-2; STIGs; Security Checklists

Techniques for security assurance conformance assessment (SACA)

Predictive Assurance

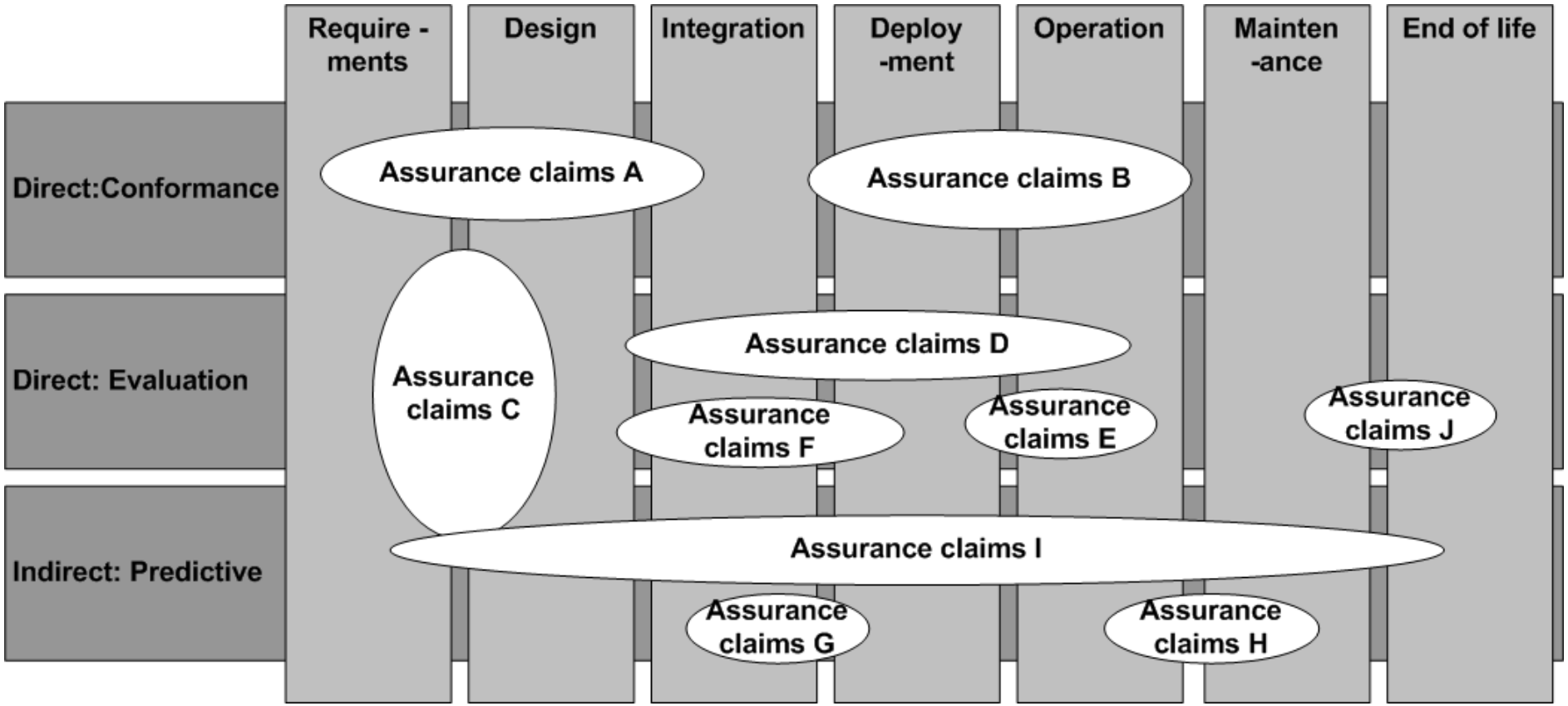
Examines environmental factors associated with the organization responsible for the deliverable are assessed. (for example a developer, integrator, vendor or operator)

These factors are dynamic and may rely on a recognized history of performance such as consistent and repeated performance to meet its security policy or to meet the assurance claims.

Many capability maturity models address predictive assurance.

Examples: SSE CMM; Site Certification of Common Criteria; CISSP

Lifecycle coverage



Composition of Assurance

- IT products are usually composed,
  - Hardware, software, firmware, liveware
  - independent assessments of some components are sometimes undertaken .
- The effects of composition on the security assurance case is an **unresolved technical problem**.
- In general, assurance authorities consider differing assurance cases as a set of disjoint assurances whose relationship is generally unknown and thus is a source of residual risk.
- Examples of properties that are hard to analyse include:
  - Information flow control
  - Fault tolerance
  - Separation

Criteria for Criteria…

Criteria for assessing schemes

- Independence
- Scheme competence
- Membership of recognition agreements and arrangements
- Assessment conformity
- Geographical considerations
- Support to security assurance users and providers
- Provision of interpretations of standards and methods
- Scheme related policies
- SACA system
- Commercial considerations
- SACA results
- SACA Marks and symbols

Criteria for the assessing assessment Bodies & Methods

Conformity Assessment Bodies

(Laboratories, Assessor Companies…)

- Independence
- Accreditation
- SACA body competence
- First, Second or Third Party

Methods

- Confidence in the assurance method
- Independent Confirmation
- Trust Policies
- Maturity of the assurance method
- Standards, Specifications and conformity assessment documents
- The standards development organization

Criteria for the assessing the assurance results

- Documentation produced
- Identification of the components of the deliverable
- Scopes and boundaries of the target of the assessment
- Functionality of the deliverable assessed
- Supply chain criteria
- Analysis of the security problem
- Lifecycle
- Operational considerations

FRITSA

- Framework for IT Security Assessment
  - An ISO Technical Report (ISO/IEC TR 15443)
  - Currently under major revision (currently at Committee Draft stage)
  - Covers the ideas included in this presentation with much more depth and explanatory material

Bibliography

- ISO/IEC 14598 (all parts), Information technology – Software product evaluation
- ISO/IEC TR 15026-1:2010, Systems and software engineering – Systems and software assurance – Part 1: Concepts and vocabulary
- ISO/IEC FDIS 15026-2:2011,, Systems and software engineering – Systems and software assurance – Part 2: Assurance case
- ISO/IEC FCD 15026-3:To be published, Systems and software engineering – Systems and software assurance – Part 3: System integrity levels
- ISO/IEC 15408:2008 (all parts), Information technology – Security techniques – Evaluation criteria for IT security
- ISO/IEC 15504:2004 (all parts), Information technology – Process assessment
- ISO/IEC 17020:1998 Conformity assessment -- General criteria for the operation of various types of bodies performing inspection
- ISO/IEC 17021:2011 Conformity assessment -- Requirements for bodies providing audit and certification of management systems
- ISO/IEC 17024:2003 Conformity assessment -- General requirements for bodies operating certification of persons
- ISO/IEC 17025:2005 Conformity assessment -- General requirements for the competence of testing and calibration laboratories
- ISO/IEC 17030:2003, Conformity assessment — General requirements for third-party marks of conformity
- ISO/IEC 18045:2009, Information technology – Security techniques – Methodology for IT security evaluation
- ISO/IEC 19790:2006, Information technology – Security techniques – Security requirements for cryptographic modules
- ISO/IEC 19791:2006, Information technology – Security techniques – Security assessment of operational systems
- ISO/IEC 23988:2007, Information technology – A code of practice for the use of information technology (IT) in the delivery of assessments
- 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
- ISO/IEC 27005:2011, Information technology -- Security techniques -- Information security risk management
- Assurance Landscape. Hopkinson, J. P.; IIT, 2007,
- CASCO,http://www.iso.org/iso/resources/conformity_assessment/objectives_and_structure_of_casco.htm
- FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems, NIST March 2006
- Software Security Assurance: A State of the Art Report (SOAR) Information Assurance Technology Analysis Center (IATAC) and Data Analysis Center for Software (DACS). July 2007
- Software Assurance Pocket Guide Series: Acquisition & Outsourcing, Volume I Version 1.1, July 31, 2009
- Suggestion for a Framework for Composite Evaluations, Helmut Kurth and Paul Karger, 5th ICCC, Berlin, 2005
- Thinking inside the box:system-level failures of tamper proofing. Saar Drimer, Steven J. Murdoch, and Ross Anderson, February 2008