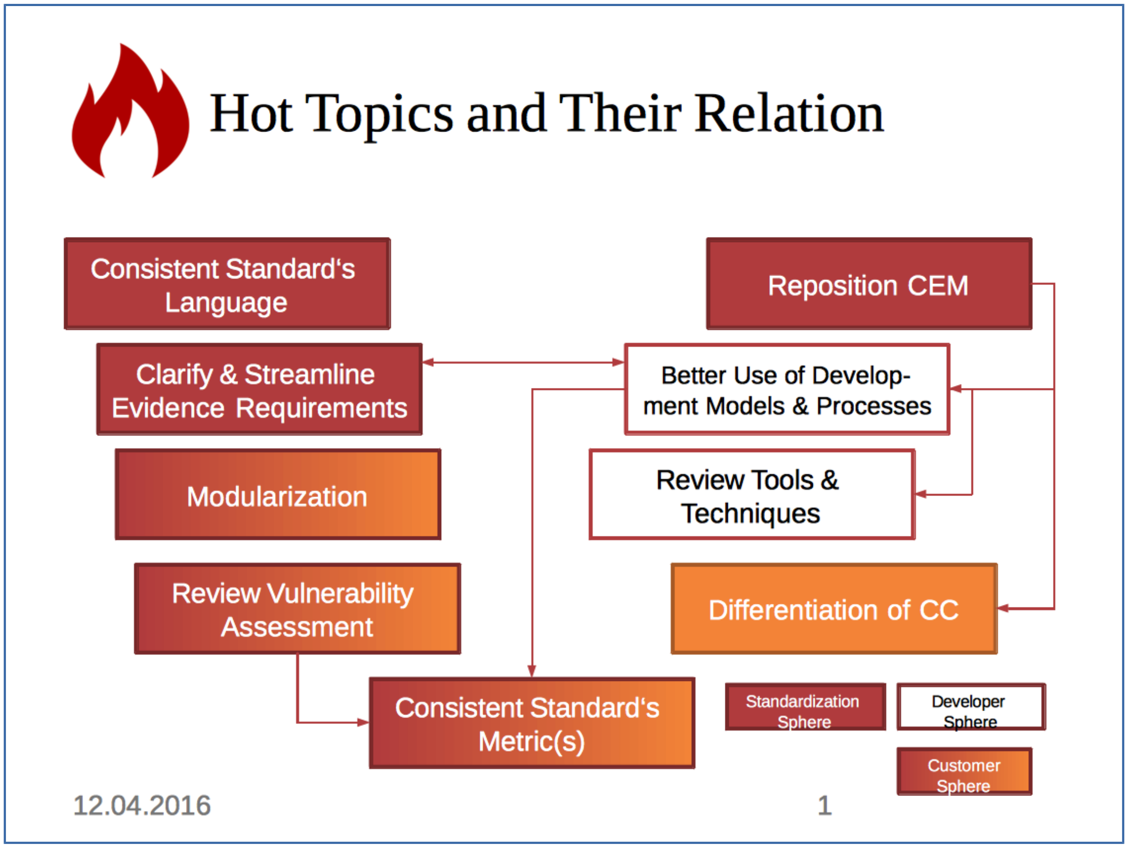
Extension of Study Period on IT Security Testing, Evaluation and Assurance Standards and Techniques (N1317) - version 1.0

Motivation

The inputs to the study period defined in N1258 "Study Period on IT Security Testing, Evaluation and Assurance Standards and Techniques" were analysed by the rapporteurs, reported in and discussed by experts during the WG3 meeting held in Tampa USA 11-15 April 2016. Some broad themes were identified which are shown in the diagram below:-



Hot Topics and Their Relation

Consistent Standard‘s Language

Clarify & Streamline Evidence Requirements

Modularization

Review Vulnerability Assessment

Consistent Standard‘s Metric(s)

Reposition CEM

Better Use of Develop-ment Models & Processes

Review Tools & Techniques

Differentiation of CC

Standardization Sphere

Developer Sphere

Customer Sphere

12.04.2016

1

The inputs all related to ISO/IEC15408 and ISO/IEC18045 either directly or resulting from aspects of their usage within recognition arrangements. The experts group considered the inputs to be highly informative and noted also that there had been informal indications that other individuals and organisations wished to provide input but had been unable to do so in the time allowed by the study period. The group therefore resolved to seek an extension of the study period and to refine the questions as below. General responses (particularly in respect of the wider aspects of the WG3 roadmap) are also welcome and the original questions are provided in Annex A.

Please Note To be as comprehensive as possible, and to provide as much background as possible for each set of questions, there is a great deal of detail provided below, together with a large number of questions. It is not expected that respondents need address all questions, rather that they select those where they have the greatest knowledge and/or concerns. Respondents could also take the questions simply as indications of some of the areas of interest and provide a more free flowing text that describes their area of expertise, any issues they see with the standards, and suggestions for improvement.

How to respond

Since there are a large number of questions under a number of headings responses to a particular question should clearly identify to which question they relate using both the section heading letter and the individual question number. For example the second question in the section "(C) Modularization" asks "Do you view this concept as useful?" - the response to this should be labelled C.2 "......."

Questions to address

(A) Consistent Standards Language

A1 Is the general model expressed in ISO/IEC 15408-1 (using users, subjects, objects, security attributes etc.) sufficient to model the security functional requirements you have? If not, what do you believe is missing or wrong?

A2 Do you believe the general structure of Security Targets and Protection Profiles defined in ISO/IEC 15408-1 is sufficient? Where do you believe it can be enhanced? Where do you believe it can/should be simplified?

A3 Has the model for the security problem definition in ISO/IEC 15408-1 using threats, assumptions, organizational security policies and security objectives been helpful? Where do you believe this model can be enhanced?

A4 Do you believe that using components from ISO/IEC 15408-2 was helpful to specify your security functional requirements? If not, where did you encounter problems?

A5 Where do you believe the functional components defined in ISO/IEC 15408-2 are inconsistent? If yes, please provide examples.

A6 Where do you believe the functional components defined in ISO/IEC 15408-2 are incomplete? If yes, please provide examples.

A7 Are there classes or families if functional components that you believe should be added to ISO/IEC 15408-2? If yes, what are those?

A8 Where did you have specific problems modeling your security functional requirements using components of ISO/IEC 15408-2? What did you do to overcome the problems (e. g. defining extended components, using refinements)?

A9 The components defined in ISO/IEC 15408-2 and ISO/IEC 15408-3 sometimes define dependencies on other components. Do you consider this a useful concept? If yes, do you believe the dependencies defined are correct and if they are not, where do you believe they are wrong and why?

A10 Do you believe that using components from ISO/IEC 15408-3 was helpful to specify your needs for security assurance?

A11 Where do you believe the assurance components defined in ISO/IEC 15408-3 are inconsistent? If yes, please provide examples.

A12 Where do you believe the assurance components defined in ISO/IEC 15408-3 are incomplete? If yes, please provide examples.

A13 Are there classes or families if assurance components that you believe should be added to ISO/IEC 15408-3?

A14 Are there classes or families if assurance components that you believe should be removed from ISO/IEC 15408-3?

A15 Where do you believe that the requirements for evidence defined in ISO/IEC 15408-3 are unrealistic? What would you suggest is a more realistic requirement for evidence for the affected assurance component?

A16 Some assurance components in ISO/IEC 15408-3 require different evidence and different evaluation activities depending on the classification of the product component into the classes 'SFR-enforcing', 'SFR-supporting', and 'SFR-non interfering'. Do you think this distinction makes sense?

(B) Clarify & Streamline Evidence Requirements

Context

The evidence requirements specified by the ISO/IEC 15408 are often not aligned with the evidence issued from the development process of the developer. Developer's evidence can often be huge. Very often "evidence" is produced specifically for the evaluation. The consequence is a significantly increased evaluation effort.

Existing evidence is rarely structured into “design”, “guidance”, “development process” and “testing” as requested by ISO/IEC 15408 but often a mixture of several of those.

However in ISO/IEC 15408, there is no explicit requirement regarding the format of the evidence (document, information, …) provided that this can be done objectively and impartially the collection of evidence is completely proper and acceptable.

A supporting CCDB Document Guidance « Collection of Developer Evidence » CCDB-2012-04-005 propose to solve some issues proposing a methodology from « creation » to « collection of evidence » with the following goals :

- minimise iterations on private/internal developer documents (it cannot be applicable to the security target or the guidance documentation of the product).
- base as much as possible the evaluation work on real documentation used by the developer and not documentation written for ISO/IEC 15408 purpose only.

The evaluator may use "Collection of Evidence" method to limit as much as possible some developer documentation written after the development. Provided that this can be done objectively and impartially the collection of evidence is completely proper and acceptable.

Key questions

Consider the many ways that evidence can be provided, through existing development practices, other assurance/certification routes etc. Reduce any pressure to produce documentation that is only for ISO/IEC 15408 evaluation. 1. Do you think that some guidance during development process can help to avoid reworking for evaluation? If so, how?

B1 In addition as well as competence of evaluator, is competence of a developer a point to address? If so how?

B2 How can the needs of users/stakeholders best be used to understand and prepare the evidence requirements?

B3 What main issues are encountered in the Evidence Requirements ?

B4 For which types and stages of development process (or site visit) have you encountered issues to provide evidence for the evaluation ?

B5 Do you think that the production of a guide to collection of evidence and/or a methodology may be useful?

B6 Can you please provide some improvements recommendation ?

B7 Which type of automated retrieval tools would you recommand ?

B8 Do you use best practices?

(C) Modularization

There are security functions that are common to many products or even many product types. Modularization is intended to address this issue allowing to define modules that combine the security problem definition, the security functional requirements, the security assurance requirements, and the evaluation methodology for such common functions in one 'module'. The advantage would be that there is a consistent method to define and evaluate such common security functions and also allow to re-use evaluation results when different products use the same implementation of such security functionality.

C1 Does the concept described above address your view of 'modularization' within ISO/IEC 15408 and ISO/IEC 18045?

C2 Do you view this concept as useful?

C3 Do you believe the current version of ISO/IEC 15408 and ISO/IEC 18045 support such a modularization concept sufficiently? If not, where do you see deficiencies in ISO/IEC 15408 and ISO/IEC 18045?

C4 Are there security functions that you see would be well suited for such a module? If yes, what do you believe are examples for such security functions?

C5 Protection Profiles are one type of modules, although they are defined to be used for a type of products. Do you think the Protection Profile concept can/should be 'widened' to also be usable for modules or do you believe modules should be defined using a different construct?

C6 There is a document on the Common Criteria Portal explaining a modular Protection Profile concept. Have you used the concept described there and if yes, what is the experience?

(D) Review Vulnerability Assessment

The amount of contributions dealing with the practice and theory of vulnerability assessment of ISO 15408 and ISO 18045 indicates the importance and necessity of this task for assurance itself and the user community.

While most contributions asked for a more consistent and less ambiguous language – covered by other hot topics, the rapporteurs found several areas concerning the design, exercise, and value of vulnerability assessment. Most of these areas are linked to other hot topics that this study period addresses:-

The area of "definition and terms“ deals with the concept of vulnerabilities as an input to the assessment and seeks for recommendations on hypothizing the quest for fundamental flaws in design, architecture, and implementation in different technology sectors.

Handling vulnerabilities in different sorts of organizational processes, and for different security needs, by means of different tools is addressed by the area "product lifecycle“.

The area of "customers' value“ seeks recommendations on the output of vulnerability assessment.

Finally, the rapporteurs open the area "responsibilities“ for ideas and best practice on how to keep patterns and concepts of vulnerabilities up to date as well as on how to strike a balance between the evaluator and certifier/validator.

Area Definition and Terms:

DA1 Do different development models and processes require a broader definition of vulnerabilities especially when evaluation is to be integrated into the development itself? Which definition would you propose?

DA2 Do the assessment's results reflect assumptions on the attacker, the source/path/entry point of an attack, and thus a risk profile to be covered?

DA3 Should the ISO 15408 empower the developer and evaluation lab to provide a rationale and justification for their hypothesis on vulnerability assessment and handling?

DA4 Are the assessment's results adequately linked to the "security promise“ of an ST, i.e. the security policy and objectives? Can an end user trace such statements of robustness and correctness back to a product's security promise and convert it into an operation plan?

DA5 Do vulnerabilities in software products induce a different/more fine-grained vulnerability definition than of hardware products?

DA6 Do you have any method for identifying vulnerabilities that has been shown to be successful (if yes, in which area, at which stage)?

Area Product Lifecycle:

DB1 How do you suggest the vulnerability assessment be handled when it must be integrated into an iterative development process?

DB2 Might penetration testing (black box testing) address all lower/commercial-level assurance needs?

DB3 Does the task of independent testing need more guidance?

DB4 Do pure software products allow for a stratified approach of flaw remediation, i.e. (immediately/shortly after recognition) remedied minor flaws and medium flaws do not revoke the certificate?

DB5 Do best practice or science provide useful metrics for evaluating vulnerabilities and flaws in order to complement/extend the CC approach of "attack potential“ vs "resistance“?

DB6 Does the differentiation into "SFR-enforcing“/ "supporting“ TSFI still support contemporary vulnerability analysis? How does that definition comply with MVC-models using callbacks?

DB7 Do you have recommendations towards reuse of results from vulnerability assessment in or from other evaluations?

Customer value:

DC1 Do customers need more guidance for their risk management in order to appropriately estimate the residual risk (remaining vulnerability) and operation of a product?

DC2 Do you have suggestions for the best way to capture the results of vulnerability assessment?

DC3 Do you have recommendations regarding reuse of results from vulnerability assessment in or from other evaluations?

Area Responsibilities:

DE1 Who should come up with an up-to-date definition and list of vulnerabilities to be looked at?

DE2 Who should set the scope and boundaries of vulnerability guidelines (schemes, developers or user communities) since databases and checklists run the risk of obsolescence?

DE3 Is it realistic to expect certified products to have no residual vulnerabilities?

DE4 Would references to other standards from ETSI or ISO for example reduce or increase the burden for evaluation labs and customers?

DE5 Who should qualify the necessary knowledge and minimum requirements to assessors?

DE6 Will all these questions be best answered through calls for expert contributions, a permanent project of ISO, or joint sessions of ISO and CCDB/CCMB?

(E) Consistent Standard's Metric(s)

The absence of performance metrics hinders the development (and use) of the standards (it is often not possible to convincingly argue what works and what doesn't).

While acknowledging that the collection of metrics in respect of effectiveness, cost, etc. of the evaluation activities relating to ISO/IEC 15408 and ISO/IEC 18045 will be performed by the ITSEF/Cerification Scheme using the standards, this study seeks suggestions for any ways in which appropriate collection of metrics could be added to the standards.

E1 What should be measured by useful metrics? (effort/cost expended, value derived - perhaps in terms of issues identified/changes made/vulnerabilities removed?)

E2 How could these be shared/collated to provide an overall view without harming intellectual property rights of the developers/ITSEF/scheme concerned.

(F) Differentiation of ISO/IEC 15408

These questions are designed to elicit information in regard to the use of ISO/IEC 15408 by stakeholders both inside and outside of the CCRA.

ISO/IEC 15408 is intended to be flexible and used in a wide variety of situations where IT Product security assurance is needed.

The questions below are intended to inquire about how the current standards meet this need.

F1 In your experience are the following markets well addressed by current certificate producing schemes? *For example :- All Government Agencies/Departments, Non-Government Agencies/Departments, Local Governments/Agencies, Critical Infrastructure, International Organizations, General Commercial, Other - Please explain.*

F2 Is using ISO/IEC 15408 validation as marketing material, demonstrating assurance to the developer's customers and potential customers a valid use of ISO/IEC 15408 evaluation?

F3 Which technology areas are not well addressed by the current standards? Please explain which technologies and what is missing?

F4 Does ISO/IEC 15408 part 1 properly address current use cases for part 2 and part 3?
For example in specifying cPPs, modularization, packages, low assurance, commercial-level assurance, High-assurance?

F5 Should ISO/IEC 15408 use cases for both evaluation and conformance be addressed?

F6 Does ISO/IEC 15408 meet the needs of other mutual recognition arrangements outside of the CCRA?

F7 Does ISO/IEC 15408 meet the needs of schemes operating outside of the CCRA?

F8 Does ISO/IEC 15408 meet the needs of commercial companies or private schemes, who may want to use CC for their own, internal, purposes?*Illustrative examples include 3GPP, EMVCo, Digital Cinema ….*

F9 Should ISO/IEC 15408-1 allow for the description of assurance activities:- For specific technologies?, On a PP by PP basis?, For ST's with no PP?, Other (Please explain)

F10 Should WG3 seek to develop liaison with any other organizations, apart from the CCDB, in regard to the future development of ISO/IEC 15408?

F11 Should WG 3 Produce any additional documents to describe use cases for ISO/IEC 15408 or other topics?

(G) Better use of Development models & Process

This section provides questions on the following topics : * Development model, * Development process and * Life cycle.

The aim is to determine what kind of changes are needed in ISO/IEC 15408 and ISO/IEC 18045 to effectively evaluate the correctness and maturity of the development process.

Questions

G1 What about the complete development life cycle?

G2 Should this topic also cover topics such as, sourcing, response, etc.?

G3 What is the value of evaluating correctness and maturity of the development process? Where is the current 15408 deficient?

G4 What are the industry leading development models that ISO/IEC 15408 should easily accommodate (e.g. Agile, Continuous Delivery, etc.)?

G5 What are current industry best practice or standards in the space of secure development process that ISO/IEC 15408 should consider (e.g. SDL, BSIMM, ISO/IEC 27034, SSE_CMM)?

G6 What are the key development activities where ISO/IEC 15408 should focus?

G7 What is the best mechanism for secure development process evaluation (e.g. derived artifact review, site visits, etc.)?

G8 When is a development process evaluation appropriate (all evaluations, lower assurance, commercial-level assurance, high assurance)? Are there multiple “tiers” of development process assurance?

(H) Reposition ISO/IEC 18045

It is clear from many of the inputs, and the discussion amongst WG3 experts that the aim of the ISO/IEC 18045 *"ISO/IEC 18045 v3.1 aims to: eliminate redundant evaluation activities; reduce/eliminate activities that contribute little to the final assurance of a product; clarify ISO/IEC 18045 terminology to reduce misunderstanding; restructure and refocus the evaluation activities to those areas where security assurance is gained; and add new ISO/IEC 18045 requirements if needed"* is often being met by the development of supporting documents (e.g. those that have been successful over many years from the Smartcard community, and those being developed by International Technical Communities (iTCs) in conjunction with collaborative protection profiles (cPPs). The role of such supporting documents for PPs leads to a number of questions:-

H1 How are such documents (which are often relatively fast changing - months rather than years)best linked to the standard in order to achieve coherence/consistency.

H2 How can those documents best support the ISO/IEC 18045 aims of *"eliminate redundant evaluation activities; reduce/eliminate activities that contribute little to the final assurance of a product; restructure and refocus the evaluation activities to those areas where security assurance is gained"* since this may involve replacing/modifying requirements in the standard.

H3 Do the 'attack potential' calculations provide value in the technology with which you are involved? Please explain why/why not

H4 How can those calculations and their underlying assumptions be better justified/tailored to the needs of a technology.

H5 Is ISO/IEC 18045 needed at all? - Would a solid link to supporting documents provide a more appropriate route for evaluation consistency?

H6 If needed how can it be improved? Please provide examples

H7 Would a guide to the production of consistent PPs and supporting documents be of value? If so please explain what you would see this covering?

Scope of Study

The scope of this study encompasses all aspects of IT product security assurance. Whilst it has a primary focus upon ISO/IEC 15408 and ISO/IEC 18045, it is most important that the result of the study period(s) also provides a good foundation for update of the WG3 roadmap and clearly identifies areas where other standards have relevance to IT product security assurance (for example ISO/IEC 27034 for product development lifecycle aspects). Comments regarding ISO/IEC 15408 and ISO/IEC 18045 may also lead to new work item proposals for additional guidance documents (e.g. a guide to the production of cPPs and supporting documents)

Expected timeframe

The working group seeks initial inputs (based around, but not limited to, the questions posed below). Responses received by 22 August 2016 will be reviewed by the working group at the UAE meeting (23-27 October 2016). The WG3 roadmap will then be updated, appropriate new work items identified, and relevant results of the study period used to facilitate review of ISO/IEC 15408 and ISO/IEC 18045 and any subsequent update (in collaboration with CCDB).

Terms of Reference

The rapporteurs will examine contributions provided during the study period and present the results to interested WG 3 experts during the next WG 3 meeting which will be held in Abu-Dhabi, UAE, according to the SC 27 calendar.

ANNEX A - Questions for the original study period

Contributions are requested on the following topics, clearly indicating the responder viewpoint (e.g. developer, end user, certification body, security consultant, etc.), and backed, where possible with clear argument/evidence:

AX1 What areas of IT product security assurance do you feel are not well covered by existing standards?

AX2 Where do the current standards work well and where should they be improved?

AX3 Is there sufficient flexibility in the current standards to be able to cover differing needs (markets/architectures/product technologies)

AX4 Where are IT vendors' current security best practices being used to demonstrate to their customers the security assurance in their products and services?

AX5 Please indicate which ISO standards such specific individually adopted best practices are mappable to.

AX6 In which areas would you use self-declaration of security from vendors, customer performed assessment, or trusted third party evaluation and certification?

AX7 Is there an effectiveness/cost limit in the depth and rigour of testing and analysis that you would be comfortable with?

AX8 How could/should robust metrics be incorporated into the IT product assurance process?

AX9 How should the development process and the evaluation be integrated to provide the appropriate level of assurance in an efficient and effective way?

AX10 How are the potentially conflicting needs for transparency of development approach/artefacts and developer intellectual property best resolved? – Is there a limit to the transparency and maturity of the development model that you would be able to accept?