Common Criteria for professionals: evaluation processes
Introduction

I have spent the larger portion of my working life doing Common Criteria evaluations and certifications, and helping/coaching/training developers, evaluators and certifiers to do evaluations efficiently. Over time I’ve given a lot of advice in many forms¹ and now I decided it was time to bring the parts around the processes together in this book.

This book takes a step back from the technicalities of the Common Criteria² and goes into the processes in a CC evaluation: the business view on the process and interpersonal view on the play between the roles of the end-user, the developer, the evaluator and the certifier.

As with the CC, these topics are quite broad and interwoven with each other. I’ve gathered them in chapters around common threads in my experience. This way the chapters can be read stand alone while showing the bigger picture.

Whom this book is written for

This book is written for people interested in improving the way a Common Criteria evaluation goes for them and/or want a view on the meta-level processes.

I’m assuming you are working in the roles of evaluator and certifier primarily, although I think experienced developers and consultants will also find it useful to know what happens in the evaluator/certifier side of the process.

I’m assuming you already have a background in Common Criteria (if you are just starting after your training in the formalities of Common Criteria, you should be fine).

Whom this book isn’t written for

This book is not written to guide developers through a Common Criteria evaluation. Should you be looking for such support as a developer, I advise you to seek consultants that have experience with evaluations, preferably in your technology field, to support you. Most of these consultants are part of the established evaluation labs and there are some like me that are independent.

This is also not for absolute beginners, as it is not an introduction book to the Common Criteria. I’m assuming you as a reader have basic knowledge of the Common Criteria, the procedures and its terms. Contrary to many books and white papers on the Common Criteria, I will not be copying in the content of the Common Criteria standard itself wholesale into this book. I consider that unnecessary padding of this book with information you as a reader should already be familiar with, or at least know how to look up.

¹ Some of you may recognize parts of this book from conversations, blog and forum posts, emails, training courses and presentations. What can I say, I’m generous in sharing and efficient with reuse.

² I’m saving that for another book.
If you do not have this level yet, you will most likely still get some valuable knowledge from reading this book, but I advise you to follow an introduction course in Common Criteria first. These are often offered by your local certification body (these are intended for beginning evaluators and tend to be highly focussed on CC-technical aspects), by evaluation labs (these range from also very CC-technical to practical for developers and that lab) and by consultants (these can typically adapted to your requirements). Obviously I provide such training too.

**Disclaimer**

As always, I stand behind my opinions and insights, as being the best way I know to explain and understand the topics. Insights can change though, as my experience grows even further. Your situation might not match the (implicit) conditions under which the described approaches are optimal. You might have completely different opinions (if so: I welcome all constructive discussion with all my heart)!³ See the chapter Contact at the end of this book or look on the [Your Creative Solution website](#).

I do know I have had to simplified things in places because the full complexity is simply too big to describe, and it is the simplified, clearer view that is most useful. Just like our teachers told us “lies to students”⁴ when they explained the earth is completely round, leaving us to discover about deformations of the globe, removing the not-so-relevant details makes the concept clearer. Only after we understood the bigger picture, we could understand and appreciate the small items that are not quite so simple. I also used that training technique in this book. I promise though, the “lies to students” are in my experience and view small items (or I will warn you for them).

As those who know me already understand: I am my own man. The opinions in this book are mine, and may or may not be those of the companies, organisations, colleagues, friends, acquaintances, and/or any sentient or non-sentient entity I have worked for, worked with, will work for/with, communicate with, compete with and/or might have been in the neighbourhood of (or not). If you have issues with something, contact me if you want to discuss it. Please do not project your opinions on my opinions onto these others.

**Dedication**

I dedicate this book to the wonderful sentient entities that have guided, prodded, challenged and otherwise supported me. With a special place of honour for DJ, for starting my growth in this domain by quickly and fully entrusting me with the ‘special’ CC projects.

---

³ Academic ground rules: for intellectual exchange of opinions, delighting in learning other viewpoints and while respecting each other. Preferably over a beer.

⁴ Adapted from the “Lies to children” part in [The Science of Discworld (2000), Terry Pratchett](#).
Common Criteria for professionals: evaluation processes

Setting context .............................................................................................................. 7
Long relationships: high switching costs ................................................................. 7

Minimal description of the CC technicalities .......................................................... 9
Example explanation of CC’s SFRs and SARs ........................................................... 9
Complexity of the Common Criteria is real ............................................................... 10
Convincing argument the CC is complex ................................................................. 10

Weight of Common Criteria .................................................................................... 12
Broad ......................................................................................................................... 12
Deep ........................................................................................................................... 12
Internationally recognised ......................................................................................... 13
Conclusion .................................................................................................................. 13

Security Target: The evaluation agreement ............................................................ 14
Changing role of the ST during the process ............................................................... 14
Changes to the ST ....................................................................................................... 15

Very rough impact of SFRs/SARs on costs ............................................................... 17

Iterations: costly ........................................................................................................ 18
A full iteration’s costs breakdown ............................................................................. 18
Reduction of amount and impact of iterations ......................................................... 19
What can the evaluator do? ....................................................................................... 19

Costs and contracts .................................................................................................. 21

Interpersonal sides of the evaluation ....................................................................... 22
Trust ............................................................................................................................ 22

Frustrations ................................................................................................................. 23
Personal contact ........................................................................................................ 23
Give the other room .................................................................................................. 23

Games inspectees and inspectors play .................................................................... 24
Dilemma sharing/client intimacy .............................................................................. 25
Risk of leakage .......................................................................................................... 26
False suggestion of knowledge and authority .......................................................... 27
Saying “pass”: the difficulty of approval.................................28
Careful with previews ........................................................................31
Contact ............................................................................................................32
Bibliography ........................................................................................................33
Games inspectees and inspectors play

The relationship between developer and evaluator, and similarly of evaluator and certifier, have both cooperative and competitive aspects on several levels. These aspects are not unique to the Common Criteria, they happen between inspectors and inspectees in the nuclear industry, pollution control and education quality [Handhaving].

In the CC evaluation process the information needs to flow from developer to evaluator to certifier. The higher the EAL, the more detailed the information becomes, leading to what in the research on enforcement of rules is called “inspectee intimacy”: the evaluators (the inspectors) know intimate details of the developer (inspectee). Similarly the certifiers will know details on the evaluators’ processes and approaches. This makes the inspectee dependent on the inspector, but also the other way around: the inspector needs the honest information to make the right decision. Together this creates two-way dependencies (for the inspector to get the information, for the inspectee to get the approval) and competition (the inspectee might like to get items approved the inspector does not want to approve).

At another level, the cooperation / competition split can also be seen in the way the inspector operates to the inspectee. In cooperative mode, the inspector tries to teach / negotiate / adapt the inspectee towards complying to the rules by explaining the goals and levels needed (this is in the literature often called the “educating inspector”), and by adapting to the specific situation of the inspectee. The underlying assumption here is that the inspectee in principle wants to comply, but does not know what he needs to comply to, or how. The relationship is considered to be important here and both forms the basis of this process and is strengthened by it.

In competition mode, the inspectee seeks to avoid complying to the requirements. A whole range of behaviour is available to avoid compliance, from hiding the non-compliance, to challenging the requirements, to challenging the competence of the inspector. The inspector in this model compensates by going to the “sanctioning inspector” mode.

As inspector (evaluator to the developer, certifier to the evaluator) one can use this cooperation / competition split as a “good cop, bad cop”-approach. Explanation of what as inspector you are looking for, what is missing to meet the criteria, and possibly examples of approaches that would meet the criteria, help the inspectee and seduce him to follow this path (the “educating inspector” as “good cop”). Backstop of the approach is the limits to which adaptations can be done. An external “bad cop” can be introduced to personify this. For evaluators this is the internal reviewer but more often the certifier, for certifiers this is the head of the scheme or colleague certifiers of other schemes.

One thing I have seen happening in myself and others as an inspector, is that the more the limits of what can be accepted are sought by the inspectee, the more your role as inspector changes from “good cop” to “bad cop”. The more the inspectee in
the view of the inspector pushes to the limits, the more the inspector starts to enforce the limits personally. In the beginning this is stated at “they will not accept this”, beyond a certain threshold it becomes “I will not accept this”.

There is a memory effect to this process: Repeated and stressed pushes to the limits makes the inspector start more in the “bad cop” sanctioning mindset. Another way of formulating this is that the worse the relationship is strained, the more strict both parties will become and will end up in a trench-warfare stalemate. In the CC stalemates are in the end, for that battle, won by the inspector: the certificate is not issued. In the long term, this causes the inspectee to avoid the inspector, with loss of work in the lab or scheme as a result.

Dilemma sharing/client intimacy

In this approach, the inspectee shows the inspector the dilemma the inspectee is faced with and invites the inspector to think with him in solving the dilemma. This approach is often fruitful in regaining the more cooperative view of the inspector and in that way is a positive strategy. A sufficient remainder of interest of the inspector to keep/regain the relationship is needed for this. By choosing the dilemma such that either solution is acceptable to the inspectee, the inspectee can try to manipulate the inspector. This “false dilemma” approach is hard to spot for the inspector. For one it is a well known rhetoric approach to focus the listener’s (inspector’s) mind on only these two options, putting the listener in the box so to say. The inspectors also generally like to feel cooperative, to be part of a solution, not just the problem.

A warning on the use of this false dilemma approach as inspectee: Even the suspicion of manipulative use of this approach can severely damage the relationship. Such suspicion is more likely to arise when the relationship is already weakened, leading to a downwards spiral that is very hard to break. Once the inspector start mistrusting every single thing you say, convincing him will be hard and ultimately much more expensive.

As inspector, the risk of going too far along in this approach should be considered. In general, my advice is to keep away from making creating the solution. A very fruitful approach is to show only the advantages / disadvantages for the options (but let the inspectee generate them), and if possible give a verdict on whether such an option would be acceptable or not.

It is best to be pessimistic and honest in these processes: a provisional “pass” verdict will be heard as a definitive one, making a change to a “fail” verdict hard to understand and accept by the inspectee. I have learned to only give “pass” estimates when there is no serious doubt, i.e. almost as a promise to pass it. If it is likely to succeed but has some doubt, explain the doubt clearly. This allows the inspectee to address this doubt, for example by generating another option right there or avoiding the failing behaviour when executing the option. Conversely,

---

16 As always with a cop-out possibility of more complete insight to fail it.
options that are almost certainly to fail should be labelled on the spot as such, preferably with explanation of what makes it fail. All other options should be labelled as “unknown” or maybe “could work, I don’t know”.

**Risk of leakage**

As inspector one has often seen the solutions of other inspectees to solve the problem at hand. It can be very tempting to show such solutions to the inspectee, especially if the solutions do not seem particularly innovative/proprietary, in a desire to seem cooperative or to co-create something (in contrast to “always failing something”). This is quickly becomes a violation of the common secrecy requirements (of the CCRA Article 5, the scheme and any NDAs between the parties) and undermines the required intimacy for effective interactions.

Especially beginning inspectees, who feel they have to catch up to the more experienced inspectees, often seek such help. I find that it is useful to explain my refusal to leak that knowledge by reflecting it back: “Let’s say I explain to you today how competitors are doing it. Tomorrow I am at your competitor <insert their nemesis>. You don’t want me to explain to them what you do, do you?”.

Another aspect of this, is that it is human nature not to be able to see the flaws in one’s own work, but easily spot them in others’ work. By co-creating the solution, as inspector you will no longer be able to adequately see the weaknesses in it. Especially with higher attack potentials this is a serious danger to the assurance.

There is a highly positive result to this approach too: I have seen time and time again that denying the knowledge of how other inspectees are solving the problem at hand, stimulates the innovation resulting in wondrous and completely unexpected out-of-the-box new solutions. Explaining what the properties are that the solution has to have to solve the problem is the key in facilitating this.

An example of a domain where I am very active: A major field of attacks in the smart card domain is side channel analysis. There is a huge set of specific attack techniques, as well as defence techniques. The attacks all depend on the combination of two aspects: an operation is performed on secret data, and via some side channel that operation leaks information sufficiently and often enough to reconstruct the secret data. Defence mechanisms seek to destroy either, or preferably both, of these aspects.

Note that this description in itself does not describe how to protect, but gives sufficient direction for designing solutions. Of course more technical knowledge such as the type of side channels available, amount and type of leakage of those side channels, etc all feeds into this, but with this information I have seen developers creating the most surprising and effective solutions.

---

17 As I write this book and polish this to my idea of perfection, I fully expect you as a reader to find all manner of mistakes and missed insights in this document I can no longer see. Please be so kind as to give me that as constructive feedback (see Contact info at the end).
False suggestion of knowledge and authority

One of the inspector strategies is “the suggestion of knowledge and authority”. Here the inspector suggests more knowledge than he actually has. I have seen this behaviour in junior and otherwise uncertain inspectors. I think this is a poor strategy within the context of the Common Criteria. It shifts away from the core idea that the inspector has to be convinced by the inspectee to give the approval (pass evaluation report/certificate). When challenged on the faked knowledge or authority, the inspector is in the situation where he can only admit not knowing (and lose a serious amount of authority and respect) or avoid that challenge by even stronger claims on his authority (further increasing the stakes). I’ve seen this process explode and been called in to repair it, it never is pretty.

In my experience it is much more productive as an inspector to use the strategy “I need to make a convincing argument and I am currently missing ... as information. Can you <inspectee> help me?”.

For the inspector the trick to this strategy is not to feel inferior, unintelligent or as a result less authoritative for not knowing the information in question. For me this rests on knowing I did all I could in keeping up with the technology developments and attack technology, leaving what I do not know as specialised and interesting knowledge to learn\(^\text{18}\). Asking the inspectee to explain it clearly to you as inspector gives the inspectee the room to show his expertise and the smart inventions. In the many times I have done this, I have never once been rebuffed or encountered difficulties in this approach and always learned something new. Simply starting the question with “I might be asking something silly as someone not coming from your domain, but <insert question>?” goes a very long way. As a side effect of being honest on not knowing, this knowledge can’t be used against you as leverage and the downwards spiral of bluffing doesn’t start.

\(^{18}\) Having genuine curiosity on that new technology/trick/method/... will help a lot in convincing the inspectee, and in a greater picture, to enjoy this work.
Contact

Obviously I welcome any questions, remarks, errata, discussion or just a thank you. By far the best way to reach me is by email to wouter@yourcreativesolutions.nl.

Catching me at a conference such as the annual International Common Criteria Conference is of course also possible. Look for me at my talk or in a lively discussion.

Thanks, errata and further information related to this book can be found on http://www.yourcreativesolutions.nl/books/.

Already thank you for the feedback and reading this book until the end!

With warm regards,

Wouter
Bibliography

The Common Criteria can as usual be found on the Common Criteria Portal <http://commoncriteriaportal.org/>.
