Common Criteria from a Commercial Perspective?
(and options for improvement with version 4.0)

Simon Milford
Head of SiVenture
What are the relationships...
Is this a viable economic model?

- **Who pays whom?**
  - Vendors pay labs
  - Vendors pay CBs (in some cases ...)
  - Purchasers pay vendors (indirectly)

- **Who benefits?**
  - Vendors, by increased sales, improved product, differentiation
  - Purchasers gain confidence in security of product
  - Labs, by having revenue
  - CBs, by having revenue

Principle benefit is not a secure product ...

It is increased confidence and reduced risk and, in some cases, access to market for the vendor
Cash flows and benefits

Is it enough to cover our costs?
Can we maintain business?

Is the risk reduction value greater than the additional cost?
Do we meet the relevant legislation?
Current Perceptions

- Good ...
  - Internationally recognised
  - Lovely places to visit for ICCC
  - Well structured
  - Clear specification of functionality (through common language CC part 2)
  - Product comparisons enabled by PPs
  - Easy to specify in procurement

- Not quite so good ...
  - In competition with other “certifications” (ICSA, West Coast Labs ...)
  - Complex, difficult to understand
  - Complex, difficult language
  - Value not understood by “man in the street”
  - Costly
  - Time consuming
  - Out of step with product development cycles
  - Not as coherent internationally as it should be
  - Already very complex (lots of work specified in CEM)
  - Much work not obviously directly related to security
Where can we go in the future?

- Keep the good bits!
  - Still want nice places to visit
  - Still want International recognition – but better!
  - Consider how to make CC n.mm Part 2 more accessible to non-experts (including the “do we still need it” option)
  - Retain technical quality
  - Take “best practice” approach to Scheme operation
  - Enable better tailoring to risk management approach

- Don’t make the bad bits worse
  - Some v4.0 proposals will increase complexity but without improving security
  - Don’t make Part 2 language any more complex!
  - Publicity drive – what can CC do for you
  - Cut out components which don’t contribute to “risk reduction”
  - Consider how life cycle can be made shorter
  - Take “best practice” approach to Scheme operation
  - Be wary of too many “national interpretations”
Requests for v4.0 and beyond …

▶ Cheaper (obviously)!
▶ More predictable costs …
▶ Better consistency across Schemes (pricing, operating model, acceptance of overseas labs)
▶ More useful results (in a risk management environment)
▶ Don’t over complicate the process (with too many assurance components, or complicated scoring systems)
Simon Milford
Head of SiVenture
Unit 6, Cordwallis Park, Clivemont Road, Maidenhead
Berkshire, SL6 7BU, United Kingdom
T: +44 (0) 1628 651 366  F: +44 (0) 1628 651 365
M: +44 (0) 7881 918 199  E: simon.milford@siventure.com
www.siventure.com