# Is the Common Criteria the only way?

*Dr. David Brewer*

*Gamma Secure Systems Limited*

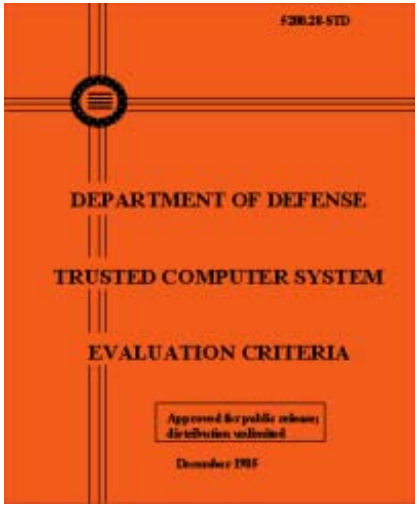
*www.gammassl.co.uk*

# Agenda

- History:
  - *CC and predecessors*
  - *Information security management*
  - *Accountancy standards*
- Pick up practical experience on the way
- Commonality and differences
- Conclusions and lessons the CC could learn

# History of CC and predecessors

# Orange Book, ITSEC, … CC




**1985**

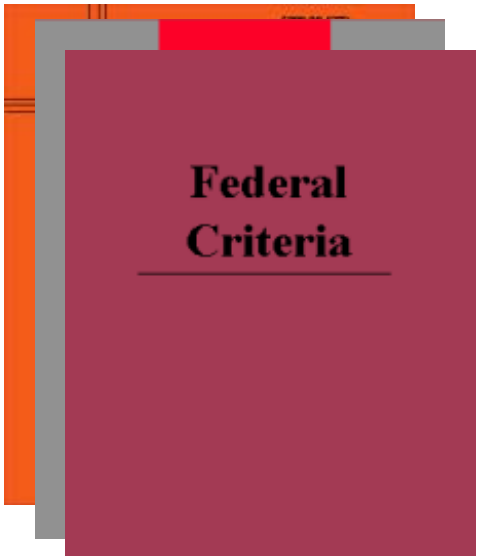
- Mid 1970's paradigm (mainframes, dumb terminals etc., Cold War threat)
- Computer security not the same as communications security
- Genre: government confidentiality, so security (basically) = access control
- Enforce security (reference monitor concept)
- Orange Book is a set of functional specifications, ranked by assurance (get it right)

# Orange Book, ITSEC, … CC


**1991**

- Mid 1980's paradigm
- Computer security and communications security have become information security
- Genre: any aspect of IT security
- ITSEC is a set of assurance specifications, free-form functionality (but had a "claims language")
- Same product assurance paradigm

# Orange Book, ITSEC, … CC




**1992**

- US response to ITSEC
- An Orange Book generation machine
- Never used

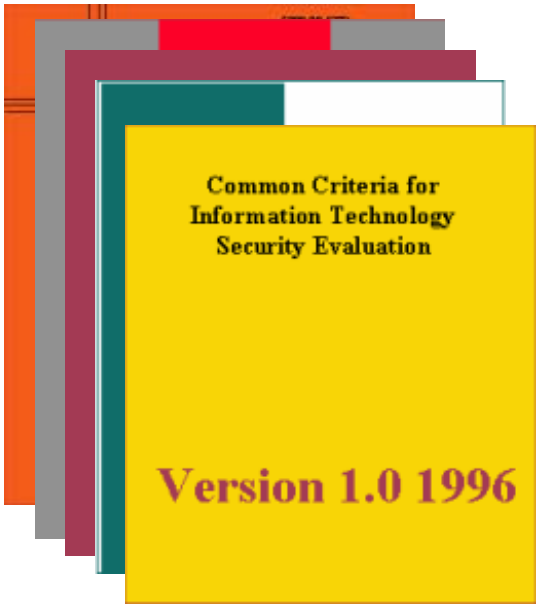
# Orange Book, ITSEC, … CC


**1993**

- Canadian response to Orange Book
- Proposed a catalogue of security functionality

Common Criteria

# Orange Book, ITSEC, … CC




**1996, …**

- Catalogues of security functionality and assurance components
- Bias towards confidentiality and ability to enforce security is still there
- Some integrity and availability but not so as well developed
- Original assurance paradigm remains (i.e. development assurance)

Common Criteria

# Vendor/User Experiences

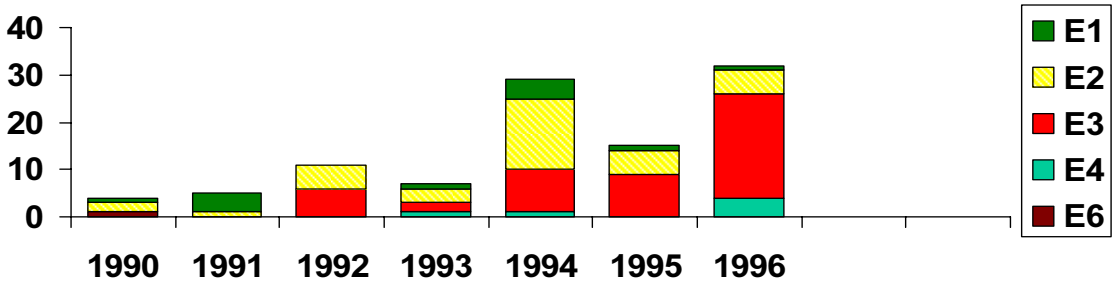
## Software Engineering

- Discipline of assurance requirements:
  - *Improved an already good development environment*
  - *Ultimate in configuration management, i.e., certificate maintenance*
  - *Outright improvement in product quality (ISO 9001)*

# Vendor/User Experiences

## Market Penetration

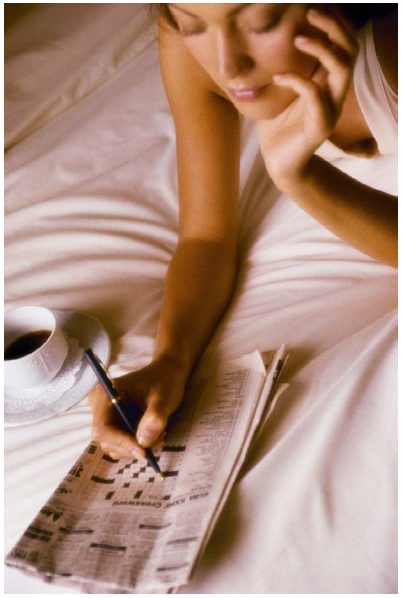
- Sudden take-up of ITSEC in 1994/5




- The Law of Leadership
  (2.5 years advantage for a US vendor)
- Enforcement helps if enforcer pays

Common Criteria

# Vendor/User Experiences



## Problems

- Time and cost, validity/scope of certification
- Mutual recognition: "evaluate once, approve everywhere" – did not work for smart cards
- APIs – Just not evaluated and are needed where product provides "take-it or leave-it" services to applications
- Composition
- Who on earth understands it?

# History of information security management and accountancy standards

# Information Security Management

- Roots in IT management community
  *(I4, ISF, BS 7799-1 (now ISO/IEC 17799:2005)*
- Guidelines for IT managers
- Led to development of management system standards *(i.e., BS 7799-2:2002, proposed to be ISO/IEC 27001)*
- Same ilk as ISO 9001/14001, i.e., part of internal control

# Accountancy Standards

- Book keeping, accounts preparation
- Auditing standards (e.g. substantive audit techniques for detecting fraud)
- Genre: "detect the event in sufficient time to do something positive about it":
  - *E.g. double entry book keeping*
  - *Systems are designed to find errors quickly*
- Accountancy Institutes have criteria for evaluating financial software packages

# Commonality, differences

# Commonality and Differences

- All are concerned with information security
- CC: IT security (predominantly platforms), biased towards confidentiality and prevention
- ISM: Covers more than just IT, embraces the Deming Cycle (Plan-Do-Check-Act)
- Accountancy: Financial applications, emphasis on detection, not prevention

# Conclusions and lessons the CC could learn

# Conclusions

- Different standards have approached the problem [information security] from different directions
- Each standard shows any given problem in a different light
- All standards have their use
- In general use an appropriate combination of standards

# Suggestion

## (for increasing market)

- ICCC4 recommended keeping CC and ISMS separate:
  - *Absolutely correct, but*
  - *ISO/IEC 17799 is a catalogue of SFRs & SARs*
  - *E.g. ISO/IEC TR 19791 (Operational System Evaluation)*
  - *Could do more regarding applications (start with APIs)*
- Bring in the concept of time-to-detect (see ICCC5)

➔ **Increase CC's utility in financial applications**

# Is the Common Criteria the only way?

*Any Questions?*

*Dr. David Brewer*
*Gamma Secure Systems Limited*
*www.gammassl.co.uk*