

Common Criteria Development – Lessons from the ISMS World

Dr. Mike Nash

Gamma Secure Systems Limited

www.gammassl.co.uk

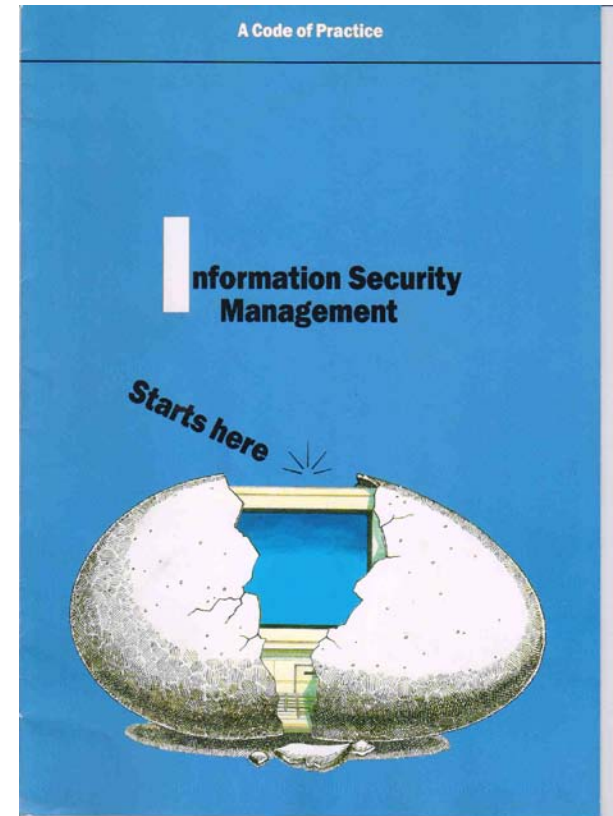
Brief History of 27000

■ Started as a UK DTI Guide

- *Not a standard*
- *Not international*
- *No certification scheme*
- *Based on key objectives*

■ Sponsored by UK Government

- *But no compulsion*
- *No CESG involvement*



Today



■ Wide series of International Standards

- *Overview (27000)*
- *ISMS Requirements (27001)*
- *ISMS Code of practice (27002)*
- *Other guidelines (2700x)*
- *Sector-specific standards (2701x)*
- *Supporting standards (2703x)*

INTERNATIONAL
STANDARD

ISO/IEC
27002

Second edition
2005-06-15

Information technology — Security
techniques — Code of practice for
information security management

Technologies de l'information — Techniques de sécurité — Code de
pratique pour la gestion de sécurité d'information

■ Certification

- *Over 5000 independently
certificated ISMS*



Reference number
ISO/IEC 27002:2005(E)

Why the success?

■ Market acceptability

- *Risk and result based*
- *Best practice but no compulsion*
- *Tells you why, as well as what*
- *Originally written by practitioners, not consultants*



■ Adaptability

- *Adoption as International Standard*
- *Multiple changes of process model*
- *Multiple restructurings of control taxonomy*
- *Disappearance of key objectives*



So what worked well?

■ Development model

- *Produced by practitioners*
- *Issued and maintained by open committee structure*



■ Public exposure of drafts

- *Fixed timetable for public comment*
- *Consensus review*
- *Every complaint must offer a solution*
- *Every formal comment must be answered*



What was also essential

■ Strategy for the way ahead

- *Internationalisation*
- *Let market demand override politics*




■ Transition Planning

- *Equivalence tables*
- *Defined transition paths*



Flexibility

- Far more organisations use certification processes than want external certification 
 - *Internal audit*
 - *Second party audit*

- Far more organisations use the Code of Practice than use the Process standard 
 - *Source of controls*
 - *“Best practice” self-assessment*

What didn't work

■ Too many cooks ...

- *ISMS standards now maintained by ISO/IEC JTC 1/SC 27/WG 1*
- *All 53 member countries of SC 27 can send delegates*
 - ❑ *Some editing groups may have 150 attendees*
- *All SC 27 member countries get one vote*
 - ❑ *Even “observers”*
 - ❑ *Example: Costa Rica and Cote d'Ivoire have same status as Canada and China*



Loss of Practitioners

- Organisations that developed the UK DTI COP:
 - BOC Group plc
 - DISC representing BSI
 - BT plc
 - DTI
 - Marks and Spencer plc
 - HSBC Bank plc
 - Nationwide Building Society
 - Shell International
 - Unilever

- Only BSI still participates in 27000 activities
 - Shell still officially a member, no activity since February 2008

Pressures

- ISMS standards are a major source of revenue to National Standards Bodies (as is ISO/IEC 15408)
 - *Some countries represented by NB employees*
 - *ISMS standards never available for free*

- Even with NB consensus endorsement, popular Working Drafts have many thousands of comments
 - *Every comment must be answered*
 - *Subconscious pressure to reject comments involving significant work*

Prestige

- All editing group participants are volunteers
- Easier to justify attendance if an office holder
 - *May also enhance career options*
- Too many standards, too many editors
 - I am a “co-editor” of 27010
 - *Not all editors have necessary experience*
 - Of writing standards
 - Of technical material
 - *Not all editors want to put in the work*

Collaboration and experience

- SC 27/WG 1 works with other industry and standards groups
 - *Sometimes very successfully*
 - *Telecommunications*
 - *Sometimes not*
 - *Medical, SCADA*

- Standards development needs experienced participants, not followers
 - *And standards must be designed for ease of use, not ease of assessing compliance*

Conclusions

- Good standards are based on practical experience
 - *And need it to gain market acceptability*
- You can change things
 - *But you have to define a transition path*
- Public participation is essential
 - *But only works if there is comprehensive feedback*
 - *Defining solutions concentrates the mind*
 - *Auditors must not define requirements*

Questions?

Mike Nash

Gamma Secure Systems Limited

www.gammassl.co.uk

Common Criteria Development – Lessons from the ISMS World

Dr. Mike Nash

Gamma Secure Systems Limited

www.gammassl.co.uk