Agenda

- Background and Philosophy
- The ISO/IEC 15408 (Common Criteria) Standard
- The ISO/IEC 17799 and BS 7799-2 Standards
- Conclusions
Background & Philosophy
Background

- US Orange Book (1985) → secure OS
- European ITSEC (1991) → any secure product
- Common Criteria (1998)
- Various codes of practice for IT systems (1987-date, e.g. German Baseline, COBIT, NIST Handbook and BS7799)
- 7799 successful because it tackles information, not just IT, and deals with security management
Philosophy

Product Certification:

- Products that can enforce security
- Demonstrate product complies with specification and no obvious vulnerabilities
- Rules for distribution and start-up

System Accreditation:

- People are non-deterministic
- Need to be able to detect events
- Dynamic Risk Management – business risks
The ISO/IEC 15408 (Common Criteria) Standard
ISO/IEC 15408

Part 1 - Philosophy

Part 2 - Catalogue of generic IT security functionality

Part 3 - Catalogue of IT developmental assurance components

CCRA Evaluation and certification scheme

Are product security claims met?
Common Criteria Approach

- **Protection Profile (PP)**: What the users want, e.g., for Visa, MasterCard etc, it is the SCSUG Protection Profile.
- **Security Target (ST)**: The vendor’s claims.
- **Target of Evaluation (TOE)**: The product itself.
- **Design documents**: Evaluation (using the Common Evaluation Methodology).
CCRA Participants

- Australia & New Zealand
- Germany
- Netherlands
- UK
- Austria
- Greece
- Norway
- USA
- Canada
- Hungary
- Spain
- Finland
- Israel
- Sweden
- France
- Italy
- Turkey

(c) Gamma Secure Systems Limited, 2003
Assurance

- 7 levels of confidence that TOE claims are correct and cannot be bypassed, deactivated, corrupted or otherwise circumvented, EAL0-7

- Another factor is strength of function, B, M, H

- Evaluation says what it was on the day

- Assurance maintenance is hard:
  - Do you want an old version that is certified?
  - Do you want the latest version, but it isn’t certified?
Application to “systems”

- Debated in Track E, ICCC4 in Sweden 9/03
- What is a system? (Willie List)
- CC dependent on product development methodology – might not work well with applications
- Overall conclusion: keep product certification separate from system accreditation
The ISO/IEC 17799 and BS 7799-2 Standards
ISO/IEC 17799 and BS7799-2

- IS 17799 is a supermarket of good things to do
- BS 7799 Part 2 is a methodology of how to use IS17799 - e.g. let’s party. Part 2 creates an ISMS
- Certification is against Part 2 - is the party OK?
Worldwide uptake

BS 7799-2 Registrations by Continent

(Click the picture for details)
ISO/IEC 17799:2000

- 10 Major Headings
- 36 Objectives
- 127 Major Controls
- Several Thousand Pieces of Guidance

(c) Gamma Secure Systems Limited, 2003
The 10 Major Headings

- Security Policy
- Security Organisation
- Asset Classification and Control
- Personnel Security
- Physical and Environmental Security
- Comms and Operational Management
- Access Control
- Systems Development and Maintenance
- Business Continuity Management
- Compliance
Security Objectives

- Secure Areas
- Equipment Security
- General Controls

(c) Gamma Secure Systems Limited, 2003
Security Controls

- Secure Areas
- Equipment Security
- General Controls

- Siting
- Power Supplies
- Cabling
- Maintenance
- Off-premises
- Disposal/reuse

(c) Gamma Secure Systems Limited, 2003
BS 7799-2:2002

- MS Standard - Explains how to apply ISO/IEC 17799

- **Build an ISMS:**
  - Management Structure
  - Define Scope & ISMS Policy
  - Risk Assessment
  - Risk Treatment & selection of controls (SOA)

- **Deploy, monitor, maintain and improve the ISMS**

- Certification is against Part 2
The Power of the ISMS

- Not just PLAN and DO, but CHECK and ACT
  - Routine Checking
  - Self Policing Procedures
  - Learning from Others
  - Intrusion Detection
  - Incident Response
  - Internal ISMS Audit
  - Management Review
  - Certification Audit

Continually checking the effectiveness of the ISMS
Certification

**EA7/03**

*Guidelines for Certifying and Registering ISMS*

Accreditation Body

**BS7799-2:2002**

*Mutual Recognition Procedures*

Accreditation Body

Accredits Certification Bodies

Certification Body

*Assesses ISMS, awards certificates in conformance with BS7799-2:2002*

ISMS

(c) Gamma Secure Systems Limited, 2003
The Real Benefits

- Security commensurate with business needs
- Integral part of the internal control system
- Reduction in insurance premium paid for project
- New customers and customer satisfaction has improved
- Senior directors ‘bought into’ the ISMS; Staff awareness is high
- Understanding of IT issues/ business risks has improved
- Security has improved; the business has improved

(c) Gamma Secure Systems Limited, 2003
Conclusion
Conclusion

- All business’s need an effective internal control system that is commensurate with business needs
  - An ISMS (BS7799-2:2002) is part of the ICS and does its job very well

- Product certification is a secondary issue
  - No point in having a certified product if you cannot detect when it has failed or is misused!

- Best therefore to deploy 7799 first and then use CC, if there is risk that an evaluated product helps mitigate.
Thank you for listening