ISO/IEC 27001: a comprehensive approach to Information Security

Computer Security Week 1st December 2006

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

Agenda

- ISO/IEC 27001
- ISO/IEC 17799
- Certification
- Case Studies
- Summary

ISO/IEC 27001 is a management system standard

ISO/IEC 17799 (27002) is a catalogue of controls you might use

Effective Security in tune with the business

Other standards concern guidance, metrics, risk assessment and certification
ISO/IEC 27001
Information Security Management Systems - Requirements

©Gamma Secure Systems Limited, 2006
Policy

ISMS Policy

- Statements to cover the requirements of the standard
- The boss wants it done that way
- Policy requirements set by a higher authority (e.g. Group HQ), as a result of their risk assessment (perhaps)
- Local policy requirements (e.g. to link to HR policy/procedures, quality policy/procedures ...)
- Statements to reduce effort later (policy does not explain why, whereas risk assessment does), e.g. “good password practice shall be followed”
Risk Treatment Plans

What is the risk?

- Proportionality → controls should be commensurate with the risk
- Decide which of the 133 controls in Annex A are applicable

Select the controls

Treat the risk
- Avoid the risk
- Accept the risk
- Transfer the risk
- Mitigate the risk

Proportionality → controls should be commensurate with the risk

Decide which of the 133 controls in Annex A are applicable
Policy/RTPs should have identified all controls, but has anything been overlooked?

- What do other people do?
- What do they do that applies to us?
- If it applies do we do it?

This is just what the SOA (Annex A ~ IS 17799) is about

- Go through all 133 controls, say whether applicable or not
- Justify by giving the reason for its selection or exclusion

SOA ↔ “Alternative Ideas” List (AIL)

It is a “safety net”
Awareness Training

- Awareness, training and competence
  - Security principles
  - Attacks
  - Policies/procedures
  - Incidents
  - Key points

Eavesdropping
- TEMPEST (computers radiate)
- Wireless networks
- Wireless telephones (no encryption)
- Stand next to a person using a mobile

©Gamma Secure Systems Limited, 2006
Incident Handling

Prompt Detection ...

- Incident Identification and Reporting
- Incident Handling and Escalation
- Communicating Results and Tidying Up
An internal ISMS audit schedule

Regularly check that controls as implemented meet policy objectives, e.g. reduce risks to the accepted level
Management Reviews

The RTP owners periodically take stock of the ISMS – is it effective?

**INPUTS**
- Results of ISMS audits and reviews
- Incident reports
- Suggestions and feedback
- New techniques, products and procedures
- Preventive/Corrective Actions
- Risk Assessment
- Results from effectiveness measurements
- Previous management review actions
- Changes affecting the ISMS
- Recommendations for improvement

**OUTPUTS**
- ISMS improvements
- Updated risk assessment
- Modified controls/procedures
- Resource requirements
- Effectiveness measurement improvements

And what about the future?
Metrics - Effectiveness

1 - \%CFES = \( \frac{TCFES}{TC} \times 100 \)
where TCFES = \( \sum \) co-workers who have received training in security, and TC = Total no. of co-workers

\( F - \frac{IPF}{TIS} \times 100 \)
where IPF = \( \sum \) Security incidents caused by lack of training, and TIS = Total no. of security incidents

1 - \%SPSM = \( \frac{TSP}{TSA} \times 100 \)
where TSP = \( \sum \) Information systems protected from malware, and TSA = Total number of systems threatened by malicious software

Guidance will be in ISO/IEC 27004 – still under development

- Detect event in sufficient time to prevent or mitigate impact
ISMS Effectiveness

Good design should ensure that ISMS detects all events in sufficient time...

May need to take action

If not there will be an impact (or near miss)

Need other checks as well

ISO/IEC 17799

Code of Practice for Information Security Management
ISO/IEC 17799

- Security Policy
- Organising Security
- Asset Management
- Human Resources Security
- Physical and Environmental Security
- Communications and Operational Management
- Access Control
- Information Systems Acquisition, Development and Maintenance
- Information Security Incident Management
- Business Continuity Management
- Compliance

Roles and responsibilities
- Prior to employment
- During employment
- Termination or change of employment

• Screening
• Terms and conditions of employment

Typical IS Events Addressed by SOA

- Theft
- Acts of God, vandals and terrorists
- Fraud
- IT failure
- Hacking
- Denial of service
- Disclosure
- Breach of the law
- Inappropriate deployment of people
Typical Business Impacts of Concern

- Adverse press coverage
- Organisation ceases trading
- Inability to carry out all or some of its business
- Loss of customer confidence
- Loss of revenue
- Increased costs
- Prosecution
- Adverse press coverage
- Organisation ceases trading
- Inability to carry out all or some of its business
- Loss of customer confidence
- Loss of revenue
- Increased costs
- Prosecution

Limitations

- Covers physical, environmental and personal security, compliance with the law etc, but ...
- ... IT component focuses on IT platforms
- There is very little on business applications
- Nevertheless scope of ISO/IEC 27001 is everything concerning information security, including the business applications
- If you want, use another AIL
CERTIFICATION

Accredited Certification

- International mutual recognition
- Desktop Audit
- Implementation Audit
- Certificate
- Surveillance

Conformance means all required management processes and applicable controls are in place and working
Non Conformities

A non-conformity "is the absence of, or failure to implement and maintain, one or more required management system elements, or a situation which would, on the basis of objective evidence raise significant doubt as to the capability of the ISMS to achieve the security policy and objectives of the organisation."

This definition comes from EA7/03

International Take-up

ISMS Registrations by Continent

5 November 2006
Mauritius

- Civil service-wide roll out
- Treasury, Civil Status, Passport & Immigration, Social Security, GOC, ...
- Plus a civil service-wide ISMS
- Covers all business applications properly
- Drive towards being a cyber island of quality
- Has significantly increased security awareness – essential for a cyber-culture
### Middle East

- Telecommunications * Petroleum
- Scope – just the IT department, so just IT not the business applications
- Need to take care because the ISMS is not responsible for everything
- Could use similar ISMS architecture as Mauritius to extend scope
- Facilitating increased awareness and tuning of policies to business requirements (i.e. not just following ISO/IEC 17799 blindly, especially where the guidance is inappropriate)

©Gamma Secure Systems Limited, 2006

### Eastern Europe

- Air traffic control
  
  Air Traffic Management Regulations
  
  ISO/IEC 27001 Annex A (the ISMS AIL)
  
  SOA (applicable controls)
  
  Non-applicable controls

- Business (air traffic control) excluded as subject to international regulations, so just IT component
- Just started – wants a market differentiator

©Gamma Secure Systems Limited, 2006
**United Kingdom**

- Fully integrated management system
- Covers all business applications properly
- ISO 9001
- ISO/IEC 27001
- Finance
- Health and Safety
- Sales and Marketing (opportunity exploitation)
- Key to running the business better

**SUMMARY**
Summary

- Comprehensive standard for information security
- Management standard (Plan-Do-Check-Act)
- Allows controls to adapt to changing circumstances (policy getting in the way of the business? – change the policy)
- Comprehensive IT-platform focussed AIL
- Increases awareness – better security – better business

ISO/IEC 27001: a comprehensive approach to Information Security

Computer Security Week 1st December 2006

Any Questions?

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