The ***Complete ISMS Toolkit***

***The* ISMS solution from your ISMS partner**

What is Information Security?

- The use of an ISMS (Information Security Management System) for the systematic preservation, in an organization, of the
  - Availability
  - Confidentiality
  - Integrity

  Of its information (and its information systems)
- Information risk
  - All information systems have vulnerabilities that can be exploited by threats in ways that can have significant impacts on the organization's effectiveness, profitability, value and long term survival
    - External threats (hackers, terrorists, viruses, spam, competitors, cyber-criminals, Acts of God, etc)
    - Internal threats – fraud, error, unauthorized or illegal system use, data theft
    - System failure – hardware failure, power outages, suppliers
- Also significant regulatory & compliance issues

© IT Governance Ltd 2005 -2008

What is an ISMS?

- A defined, documented management system (within a defined organization, the 'scope')
  - A board information security policy
  - A corporate risk treatment plan
  - An inventory of information assets (data and systems) that fall within the scope
  - An assessment of vulnerabilities, threats and risks ('risk assessment') to those assets
  - A Statement of Applicability identifying a set of controls (responses to/counters for risks) that respond to the risks
  - A comprehensive suite of processes, policies, procedures & work instructions
- The ISMS must be
  - Implemented and managed
  - Reviewed, audited and checked
  - Continuously improved
- Certification
  - Valuable but not always essential
  - The final stage
  - Carried out by a third party certification body
  - Evidence as to the completeness and quality of the ISMS

© IT Governance Ltd 2005 - 2008

What are BS7799 and ISO17799?

- Two interlinked standards
  - ISO27001 specifies how to design an Information Security Management System ('ISMS')
    - How the ISMS should work, not what should be in it
    - Replaced BS7799
  - ISO27002:2005 is an international code of practice for information security best practice that supports and fleshes out ISO27001
    - What should be in the ISMS, not how it should work
- Management system standards
  - Technology agnostic
  - Non-technical
  - Non-jurisdictional
  - Conceptually similar to ISO9000
- Internationally understood
- Capable of external certification
- Commonly accepted best practice
- 200+ new ISO27001 certifications/month

© IT Governance Ltd 2005 - 2008

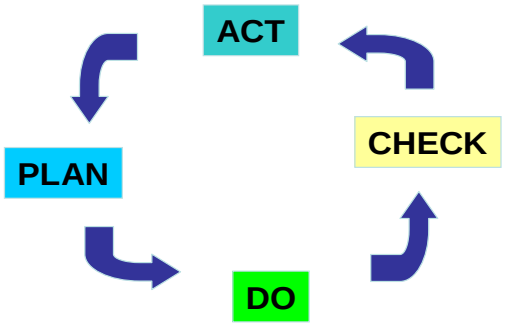
Business drivers

1. Implement information security best practice
    - Security of corporate information assets
    - Protection of corporate reputation
    - Meet governance and regulatory compliance requirements
    - Improvement in effectiveness of corporate IT infrastructure
    - Corporate quality assurance
2. Drive for certification
    - Demonstrating best practice
    - Corporate positioning
    - Customer/partner requirement
    - Government/funder requirement
3. A combination of the above
    - 1 & 2 are not incompatible!

© IT Governance L td 2005 - 2008

How do we create an ISMS?

- PDCA



PLAN

- **Identify assets, scope, carry out risk assessment, create policies, processes**

DO

- **Implement the defined and agreed processes**
- **No action required for accepted risks**

CHECK

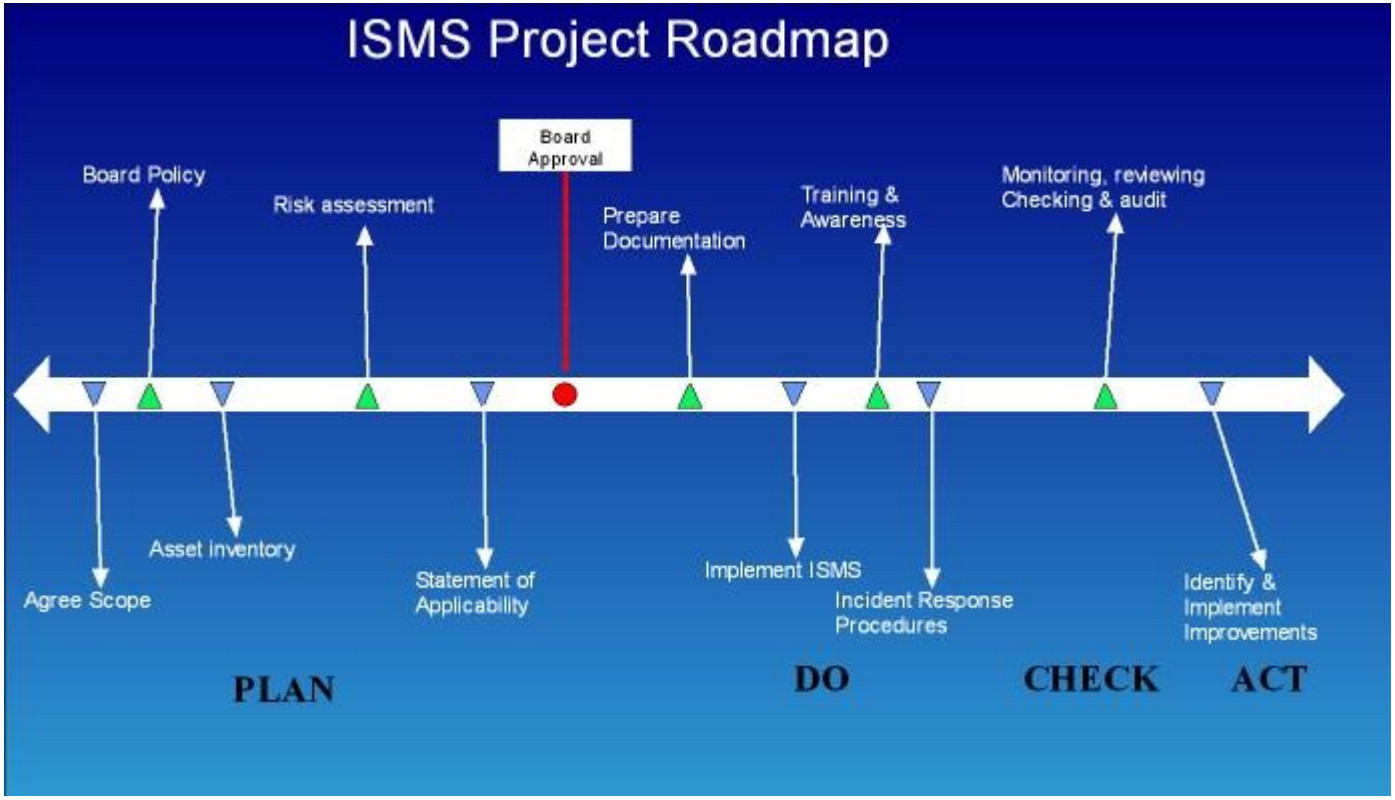
- **Assess performance against defined policies**

ACT

- **Take corrective and preventive action to continually improve the operation of the ISMS**

© IT Governance Ltd 2005 - 2008

The ISMS Project Roadmap



© IT Governance Ltd 2005 - 2008

ISMS Documentation Requirements

- Must be company-wide
- Must be cross-functional
- Must be management-led
- Will have significant internal linkages and cross-references
  - Essential for effectiveness, internal coherence and consistency
  - Must ensure there are no information security gaps
- Must comply with ISO27001specification
- Must reflect ISO27002:2005 guidance
- Requires four levels of documentation
  - Board approves level 1: Corporate policy, risk treatment plan, Statement of Applicability (134 controls), ISMS manual
  - Executive approves level 2: procedures
  - Line managers approve level 3: operations/work instructions
  - Level 4 documents are records that do not need approval
- Must reflect Plan-Do-Check-Act (PDCA) cycle
- Must be continuously improved

© IT Governance Ltd 2005 - 2008

Two project approaches

- Sequential mini-PDCA cycles
  - Tackling either sub-units (divisions, geographies, etc) of the whole organization or specific control areas (prioritized through a high level risk assessment)
- Massively parallel implementation
  - Designed to get the whole organization to project completion quickly and completely
- Issues:
  - Procedure overlap, procedure and work instruction cross-referencing
    - one work instruction or procedure may need to meet the requirements of a number of controls
    - One control may require a range of procedures and work instructions that affect a diversity of functional areas within the organization
    - Each procedure and work instruction needs to be aligned with all the others, for coherence and consistency and to ensure there are no security gaps
  - **Only the ITG *Complete ISMS Toolkit* enables an organization to proceed safely with either approach**
    - Overlaps identified and dealt with
    - Cross references already in-built
    - All policies, procedures and work instructions are aligned
    - Internal coherence and consistency is assured
    - All tools designed to be interoperable

© IT Governance Ltd 2005 - 2008

Time to certification/completion

- In a mid-size company that already has a reasonable security posture
- Massively parallel approach
- Assuming management commitment, project prioritization, training and adequate resourcing
  - 'DIY' approach
    - Time required: 14 – 19 months
  - Consultant-led approach
    - Time required: 10 – 14 months
  - ITG Fast Track approach
    - Time required: 8 – 12 months

© IT Governance Ltd 2005 - 2008

‘DIY’

- Methodology: trial and error
- Average time to completion: 14-19 months
  - understanding requirements: 1 month
  - Project planning: 1 month
  - Drafting corporate policy and project team training: 1 month
  - Risk assessment and Statement of Applicability: 2 months
  - Drafting procedures: 3-5 months
  - Drafting operations/work instructions: 4-8 months
  - Implementation (Do), audit and review (Check) and improvement (Act): part parallel, plus 2 months
- Disadvantages:
  - Time requirement
  - Absence of best practice
  - Uncertain PDCA cycle
  - Likely to be inadequately led, not cross-functional, not company-wide
  - High likelihood of project failure
  - Continuing, real Information Security exposures

© IT Governance Ltd 2005 - 2008

Consultant-led

- Methodology: deploy external expertise
- Average time to certification: 10-14 months
  - Understand policy: 1 week
  - Project planning: 1 week
  - Drafting corporate policy and project team training: 1 month
  - Risk assessment and Statement of Applicability: 2 months
  - Drafting procedures: 2-4 months
  - Drafting operations/work instructions: 3-5 months
  - Implementation (Do), audit and review (Check) and improvement (Act) in parallel, plus 2 months

- Advantages:
  - Faster
  - Will contain some best practice
    PDCA cycle and cross-functional, company-wide requirements should be met-
  - Reduced likelihood of project failure
- Disadvantages:
  - Extensive consultant time, expense
  - No continuous improvement
  - Continuing, real information security exposures

© IT Governance Ltd 2005 - 2008

ITG Fast Track

- Methodology: deploy IIT Governance Complete ISMS Toolkit
- Average time to certification: 8-12 months
  - Understand policy: 1 week
  - Project planning: 1 week
  - Drafting corporate policy and project team training: 1-2 weeks
  - Risk assessment and Statement of Applicability: 2-4 weeks
  - Drafting procedures: 4- 6 weeks
  - Drafting operations/work instructions: 2-4 months
  - Implementation (Do), audit and review (Check) and improvement (Act) in parallel
- Advantages:
  - Fit for purpose – designed to meet ISO27001/ISO27002 requirements from the outset
  - Fast to deploy
  - Very cost-effective (with low TCO and high ROI)
  - Full of best practice
  - Will be cross-functional, company-wide, with correct PDCA cycle
  - Very low likelihood of project failure
  - Continuous improvement built in from the start
- How?
  - Massively parallel documentation drafting
  - Multiple mini-PDCA cycles made possible by interlinked documents
  - No trial and error –very little review, revision and correction required
- Additional support:
  - ISMS Implementation Master Class
  - Specialist consultant oversight and guidance

© IT Governance Ltd 2005 - 2008

What is the ***Complete ISMS Toolkit***?

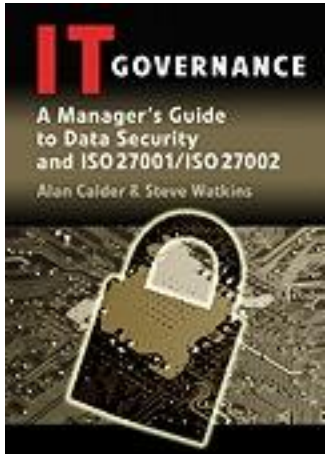
- Standard templates with pre-written content
  - Abstracted from multiple, successful ISMS deployments
  - With line-by-line instructions for, and guidance on, completion
- Includes:
  - Draft corporate policy (level 1)
  - Draft Statement of Applicability, ISMS manual and policies (level 1)
  - Draft of every procedure likely to be required (level 2)
  - Operations/work instruction templates (level 3)
  - Correct PDCA cycle
  - Project tools included in the price
    - Risk assessment/gap analysis tool
    - Training slides
    - Audit checklist
- Supported by:
  - Detailed guidance of "IT Governance: a Manager's Guide to Data Security and ISO27001/ISO27003" (4th edition)
    - see www.itgovernance.co.uk/products/4
    - "A comprehensive guide as to actions that should be taken." Nigel Turnbull, Chairman, Lasmo plc, author of the Turnbull Report.
  - Online access to additional, current material, including a glossary
  - UNIQUE e-mail fast response drafting support
  - Ongoing Toolkit upgrades

© IT Governance Ltd 2005 - 2008

Open University

- The Open University's post-graduate course on information security management for information security professionals. M886: Information Security Management is based on "*IT Governance: a Manager's Guide to Data Security and BS7799/ISO17799*" (3rd edition)
- www3.open.ac.uk/courses/bin/p12.dll?C02M886

- "*The Calder and Watkins book underpins professional practice in InfoSec Management. Following the standard, risk management guidance is given for each InfoSec area, including the trade-offs that arise between covering a vulnerability and leaving it uncovered. For complete coverage of the standard, this book is unparalleled, and that's why we have chosen it as the basis for the Open University's new Information Security Management Course.*" Dr Jon G Hall, Lecturer in Information Security, Open University, UK



© IT Governance Ltd 2005 - 2008

Who are IT Governance Ltd?

- Governance, risk management, compliance and information security specialists
- Deep expertise in management of governance, quality systems, information technology and information security
- Multiple successful ISMS deployments in both public and private sectors
- Certification body and ISMS international user group members
- Delivering a growing range of IT governance and information security books, tools and support services
- Strategic approach to product development
- Fostering long term client relationships

© IT Governance Ltd 2005

What next?

BUY ONLINE

- Standalone Documentation Toolkit - just the ISMS documentation, or

- The No 4 ISMS Toolkit contains, in addition to the Documentation Toolkit,
  IT Governance: a Manager's Guide to Data Security and ISO27001/ISO27002, 3rd edition (ITG4)
  A comprehensive online information security glossary

- The No 5 ISMS Toolkit contains, in addition to the contents of the No 4 Toolkit,
  Copies of both ISO 27001 and ISO 27002

- The No 1 ISMS Toolkit contains, in addition to the contents of the No 5 Toolkit,
  BS7799-3, the risk assessment standard

- The No 3 ISMS Toolkit contains, in addition to the contents of the No 1 Toolkit,
  vsRisk™, the definitive ISO27001 risk assessment tool

- The No 2 ISMS Toolkit is the same as the No 3 Toolkit, except that it doesn't contain
  the three information security standards.

ALSO CONSIDER THE ISO27001 ISMS IMPLEMENTATION MASTER CLASS

© IT Governance Ltd 2005 - 2008