



ctg

using

ISO 27001

to your advantage

Topics

- Overview of ISO 27001
 - History
 - Trends
 - Basics
- ISO 27001 in the real world
 - Threats
 - How an ISMS is used
 - Where it's making a difference
- Q & A

A photograph of a modern meeting room with a long, polished conference table, several leather chairs, and large windows overlooking a cityscape. A green plant is visible in the background.

Overview of ISO 27001

History

The ISO 27001 Series

- ISO/IEC 27001:2005
Information technology – Security techniques – Information security management systems – Requirements
- ISO/IEC 27002:2005 (17799:2005)
Information technology – Security techniques – Code of practice in information security management
- Others (mostly) to come...

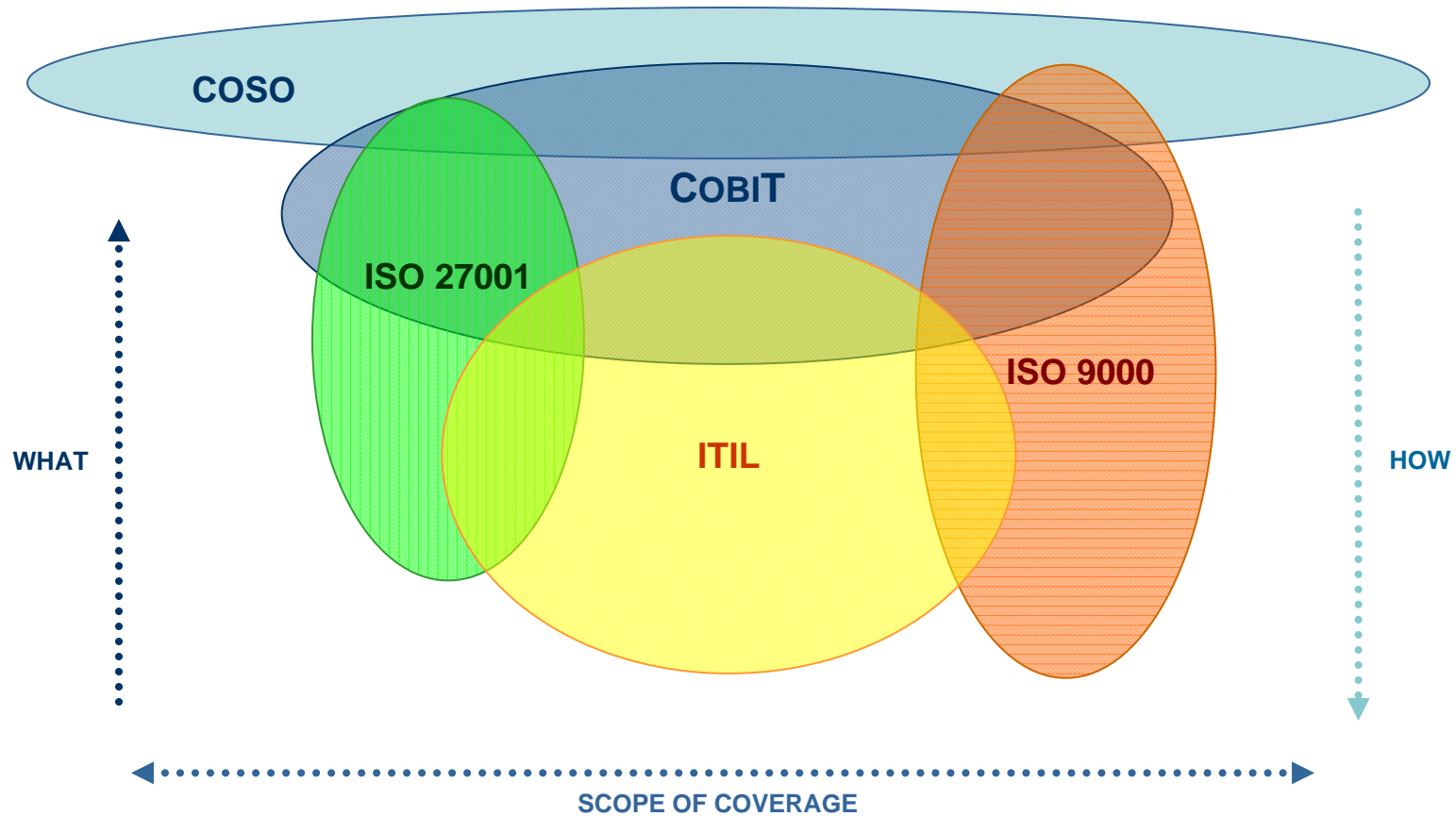
Where Did 27001 Come From?

- ISO
 - International Organization for Standardization
 - Non-governmental organization
 - 157 member countries
 - Geneva, Switzerland
 - 16,500 standards since 1947
 - Soap (6387:1983) to nuts (ISO 16950:2003)
 - Kitchen sinks (ISO 3055:1985)
- IEC
 - International Electrotechnical Commission

How Did 27001 Get Here?

1992	UK's Dep't of Trade & Industry (DTI) publishes <i>Code of Practice...</i>
1995	British Standards Institute (BSI) amends and republishes as BS7799
1998	BS7799-2 published
1999	BS7799-1 revised, LRQA and BSI become first certifying bodies (CBs)
2000	BS7799 is "fast-tracked" to become ISO/IEC 17799
2002	BS7799-2 revised to incorporate Deming (PDCA) cycle
2005	New version of ISO 17799 published, ISO 27001 published
2007	ISO 17799 renamed to ISO 27002

Where Does 27001 Fit?



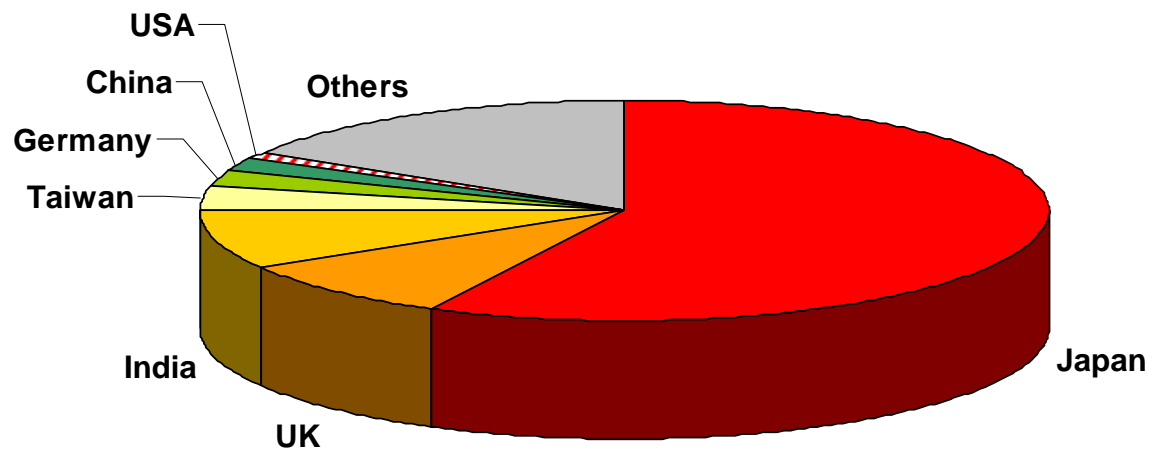
The background of the slide is a photograph of a modern meeting room. It features a long, polished wooden conference table in the foreground, with several brown leather chairs arranged around it. A green plant in a pot sits on the table. Large windows in the background offer a view of a city skyline under a clear sky.

Overview of ISO 27001

Trends

Global Adoption

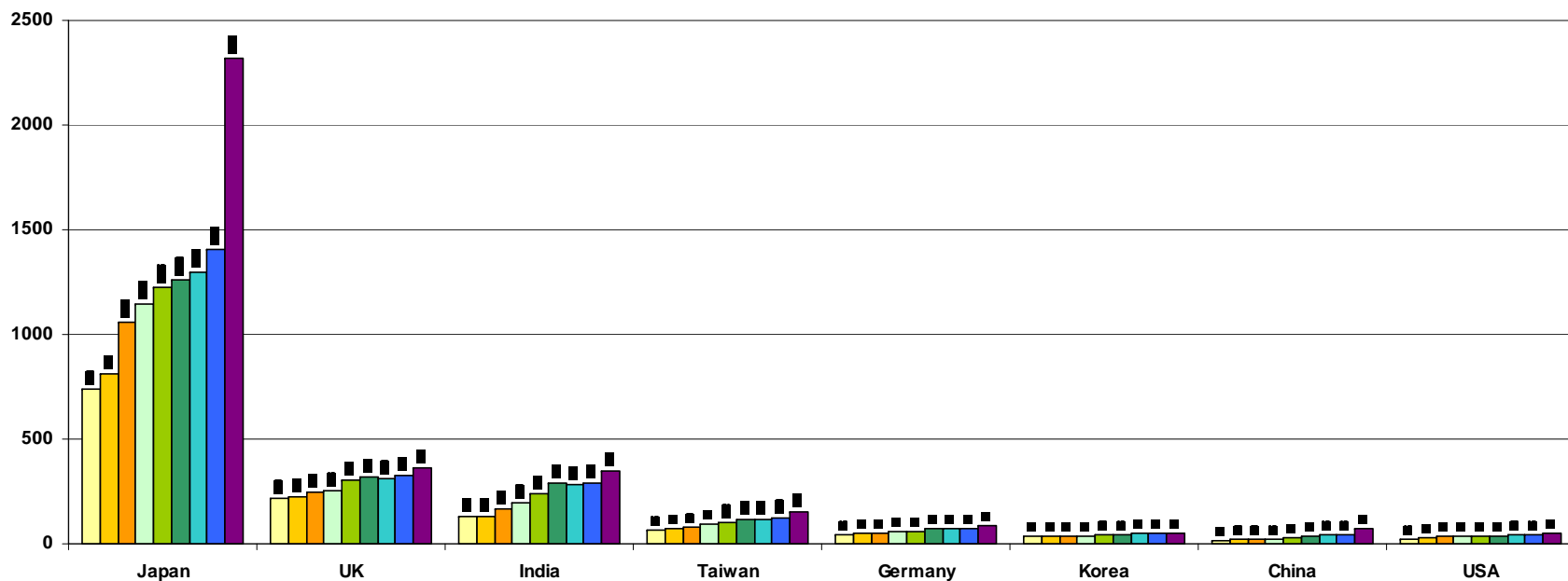
- Japan 58%
- India 9%
- UK 9%
- USA 1%



* International Register of ISMS Certificates (December 2007)

Growing Acceptance

- ISO 27001 global certificates (10/2005-12/2007)



* International Register of ISMS Certificates (December 2007)

Overview of ISO 27001

Basics

“Information”

- Types
 - Printed
 - Written
 - Mailed
 - Stored electronically
 - Transmitted electronically
 - Video
 - Spoken in conversation

“Information”

- Information assets
 - Created in the course of business
 - Created using applications
 - Software
 - Facilities and equipment

“ISMS”

- Information Security Management System
 - Top-down, business-driven approach
 - Risk-based
 - Preserve confidentiality, integrity, availability
 - Physical and electronic assets
 - Not just controls – it’s the process
 - Establish, implement, operate, monitor, review, maintain, and improve
 - Managing documents and records

What is Included?

- Scope
 - Business
 - Organization
 - Location
 - Assets and technology
- *Not* an IT-only standard
 - There are no technology requirements – for example, “firewall” isn’t mentioned
 - There *are* IT-related controls

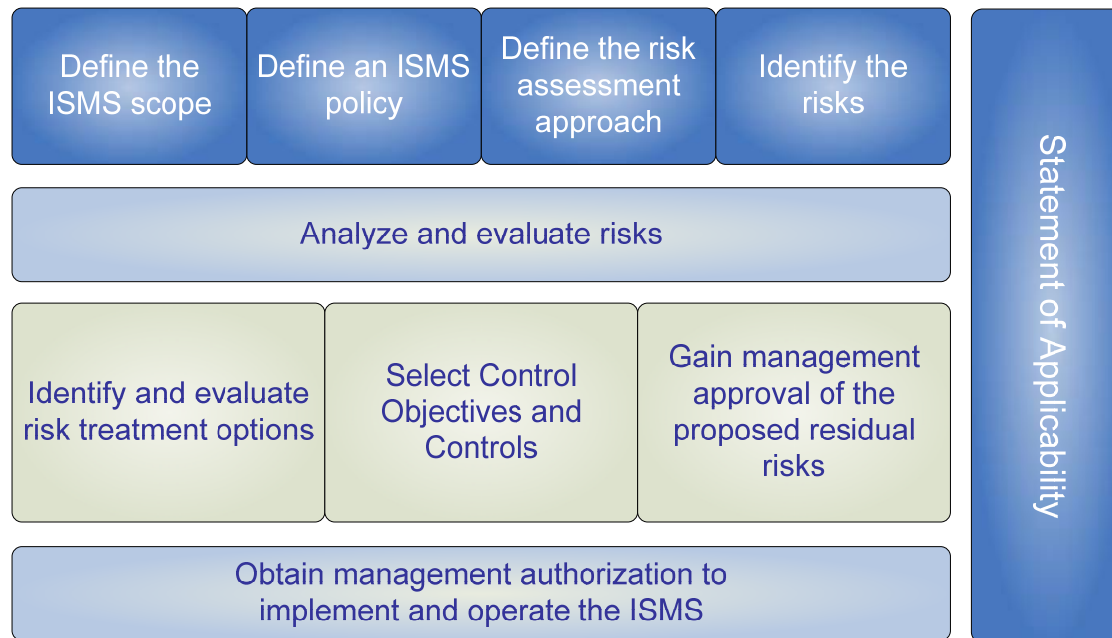
27001's Management Principles

- Leadership
- Customer focus
- Involvement of people
- Process approach
- System approach to management
- Continual improvement
- Factual approach to decision making
- Mutually beneficial relationships

PDCA Model



Establishing an ISMS (“Plan”)



Implement and Operate (“Do”)

- Execute risk treatment plan
- Put policies and procedures to practice
- Implement training and awareness
- Manage incidents
- Create records
 - Management decisions, actions, results
- Control documents and records

Monitor and Review (“Check”)

- Measurement
 - Technical and program metrics
 - Events and incident management
- Assessment and audits
 - Compliance with policies
 - Technical assessment
 - Regulatory and standards requirements
 - Internal ISMS audit

Maintain and Improve (“Act”)

- Regular management reviews
 - Look at “input” from monitoring, audits, risk assessments, etc.
- Review policies and controls
- Review residual risk
 - Evaluate established acceptable risk level
- Implement improvements
 - Corrective and preventative actions

Benefits of ISO 27001

- Create a competitive advantage
 - Satisfy customer requests, RFPs
- Avoid chasing compliance
 - Single approach to legal, regulatory drivers
 - Easier regulatory/audit reporting
- Improve visibility into security program
- Avoid breaches – protect reputation

(More) Benefits of ISO 27001

- Avoid “zero tolerance” security
 - Program based on risk
 - Avoid unnecessary controls
 - The *right* people, processes, and technology to protect information assets
- Reduce ROI (risk of imprisonment)
 - Due diligence
 - Reduced liability risk

ISO 27001 in the Real World

Case Study: Breaches

Privacy Rights Clearinghouse

- 839 reports since January 2005
- Top offenders:
 - Universities (24%)
 - Financial services (13%)
 - State government (10%)
 - Federal government (8%)
 - Hospitals (7%)
 - Retail (6%)

Privacy Rights Clearinghouse (cont'd)

- Top breach types:
 - Stolen laptop (21%)
 - Hacking (20%)
 - Web hacking (15%)
 - Fraud (6%)
 - Stolen computer (6%)
 - Document disposal (5%)

* Additional data sourced from attrition.org.

2007 Mishap of the Year

- Impact
 - Wireless network (WEP) at two FL stores
 - Later access to internal systems (for 18 mos.)
 - 47.5 to 94 million credit/debit cards
 - \$68-83 million in fraud in 13 countries
 - Aftermath:
 - 19 lawsuits plus FTC and 37 state AGs
 - \$256 million est. cost to company (8/2007)
 - \$40.9 million to banks/card brands (11/2007)

Did the company have an ISMS?

- No.
 - It didn't apply controls appropriate to the risk
 - It did not detect the attack
 - It did not detect the continued activities by attackers between mid-2005 and Dec. 2006
 - It stored sensitive credit card data
 - It did not have logs to determine what had happened once the attack was discovered

Boosting Confidence in Security...

- An ISMS helps you to not be the next
 - Implementation
 - Identify your assets
 - Assess the risks to those assets
 - Apply appropriate controls to protect your assets
 - Training and awareness
 - Monitoring
 - Controls are in place to monitor systems
 - Metrics are defined, tracked, and reported

ISO 27001 in the Real World

Case Study: Competition

Manufacturing/Services Company

- Global document management company
 - 8,000+ employees
 - Multiple ISMSs globally
- Drivers for implementation
 - Corporate goal to establish ISMSs
 - RFPs asking about ISO 27001 compliance

Creating a Competitive Advantage...

- ISMS
 - Tangible evidence via certification
 - Clear response to RFPs on security practices
- Other benefits
 - Risk assessment identified areas where improvements were needed
 - Staff now understand security responsibilities
 - Identified processes that could be simplified or eliminated

ISO 27001 in the Real World

Case Study: Budget Justification

Beverage Company

- Trade secrets are its “crown jewels”
 - “Information is the life blood of the company”
- Incident
 - Employee offered formula and development sample to competing company

Corrective Actions

- The response of the ISMS
 - Review information protection policies, procedures, and practices
 - Are safeguards for IP adequate?
 - Make improvements
 - Updated personnel controls – e.g., frequency of background checks – for high-risk roles
 - Adjust spending to account for changes

Justifying Spending...

- Budgeting for reality
 - Process connects spending to business needs
- Good practice
 - Costs based on easily defensible framework
 - Budgets linked to clear security objectives
- Risk assessment
 - Security risks are presented to management
 - Risk treatment plan ties spending to risk



ISO 27001 in the Real World
Case Study: Reducing Cost

U.S. State Government

- Executive branch
 - 10,000+ employees
- Drivers for use of ISO 27001
 - Haphazard collection of policies
 - Many compliance requirements
 - HIPAA, PCI, state and federal mandates
 - Interest in integrating NIST guidance
 - Agencies looking for direction

Rationalizing Compliance Efforts...

- ISO 27001 becomes focal point
- Requirements map to ISMS controls
 - Cross-referencing is used to connect policies to controls, controls to regulatory drivers
- Single set of policies, procedures
 - Shows how policies based on good practice meet regulatory requirements rather than writing policies specific to each regulation

Reducing Costs...

- Unifying compliance efforts
 - HIPAA, GLBA, SOX, PCI DSS, SAS 70, state breach disclosure laws
- Reducing audit effort
 - Streamline production of audit evidence
- Extensible framework
 - Extend to all agencies in executive branch
 - Share with legislative, judicial branches



Q&A

“Ask the Auditor”