Information Security Compliance for Sarbanes-Oxley and Basel II

Computer Security Week 30th November 2006

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

Certificate No. IS 85916 Certificate No. FS 30710

Agenda

- Laws and regulations
  - *Sarbanes-Oxley*
  - *Basel II*
- The impact of IT
- A management issue
- ISO/IEC 27001 – *an information security management system standard*
- Compliance
  - *Internal control*
  - *SOX – traceability of financial transactions*
  - *Basel II – measurement of operational risk*
- Internal control
- Summary and conclusions

Sarbanes-Oxley

- An act "to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the security laws, and for other purposes"

Same for all laws/regulations concerning corporate governance

- Places heavy emphasis on internal control, e.g.
  - *§404 (a) (1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting.*

Easier in the days of the quill pen – but not so in the information age

Basel II

- Extends credit/market risk provisions of Basel 1 to operational risk
  - *The risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems, or from external events*
- Encourages establishment of effective internal control to release Tier 1 capital
- Can you demonstrate effective control to satisfaction of the regulators?

The impact of IT

- Remote access – potentially anyone can change the books
- IT is very complex – how do you know that it is working?
- We rely on IT – what do you do when it breaks?
- IT keeps changing – can you still read records you made a few years ago?

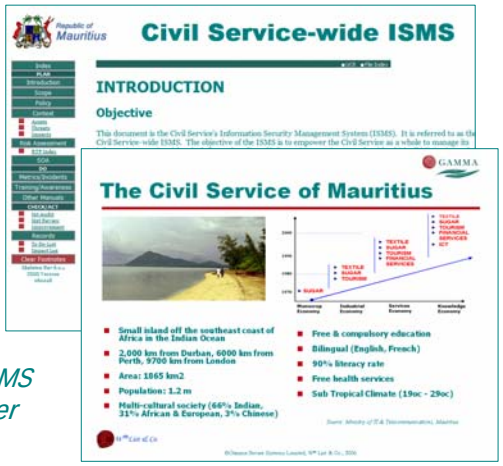
A management issue

- What if business practice change?
- What if there is a new threat/regulation?
- What if someone makes a mistake?
- What if there is an unprecedented disaster?
- Technology is not the answer
- What you need is a “management system”

ISO/IEC 27001

Information Security Management Systems - Requirements

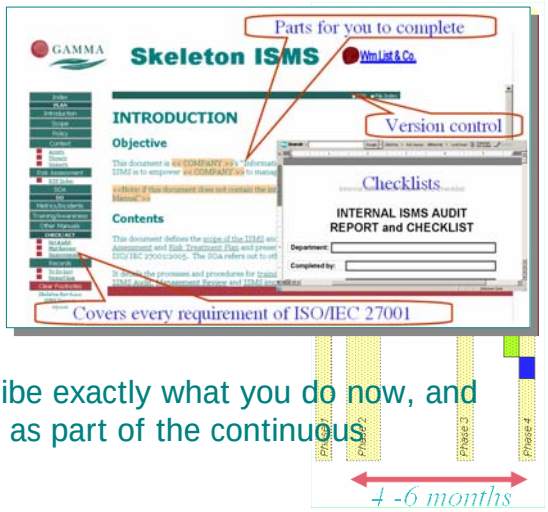
International take-up



- Mauritius:
  - *Civil service-wide roll out*
  - *Treasury, Civil Status, Passport & Immigration, Social Security, GOC, …*
  - *Plus a civil service-wide ISMS*
  - *Drive towards being a cyber island of quality*

Easy to implement

- Skeleton ISMS
- Event-impact RTPs, performed by senior managers
- Integrate with existing internal control structures



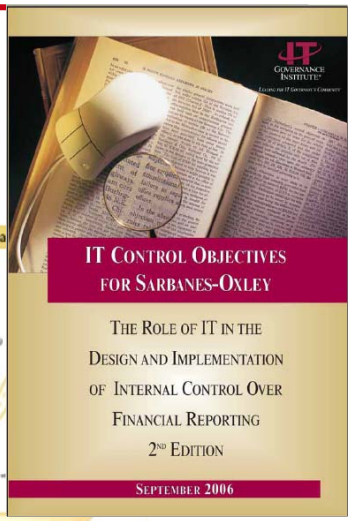
- Build an ISMS to describe exactly what you do now, and treat your future plans as part of the continuous improvement cycle

Compliance

- ISO/IEC Annex A controls focused towards IT platforms
- Super start but need more than that:
  - *SOX – traceability of financial transactions*
  - *Basel II – measurement of operational risk*
- Internal control has different meanings around the world, e.g.:
  - *In US – only financial reporting*
  - *In UK - everything*

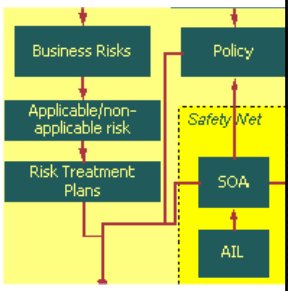
SOX – ITGI's CobIT

- Not a management system, but...
- Useful guidance
- Control objectives
- Alternative ideas
- Just like Annex A to ISO/IEC 27001 but focused on financial applications



Different AILs

- Policy/RTPs should identify all required controls
- But has anything been overlooked?
- Go through the "Alternative Ideas" List (AIL) to find out
- Document results in the Statement of Applicability (SOA)
- The AIL acts as a "safety net"
- IS 27001 Annex A, ITGI are examples

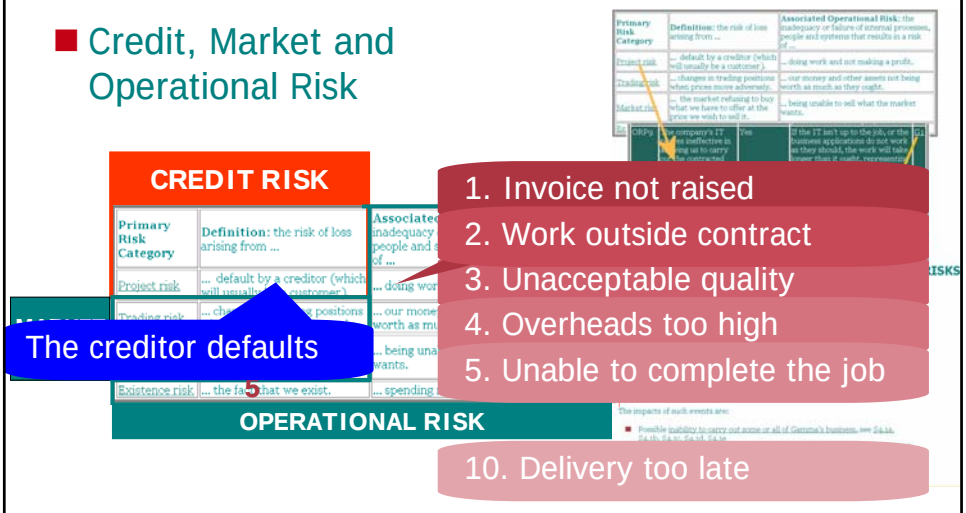


Basel II

- Credit, Market and Operational Risk

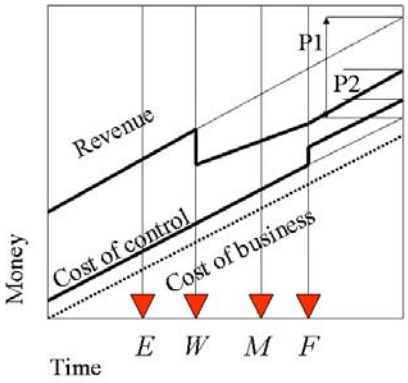
Basel II

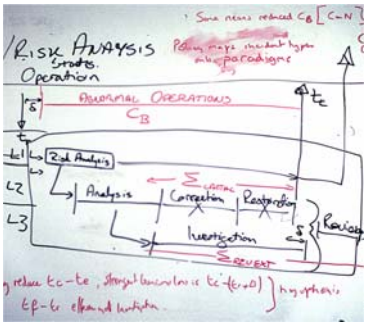
- Credit, Market and Operational Risk



©Gamma Secure Systems Limited, 2006

Measuring effectiveness

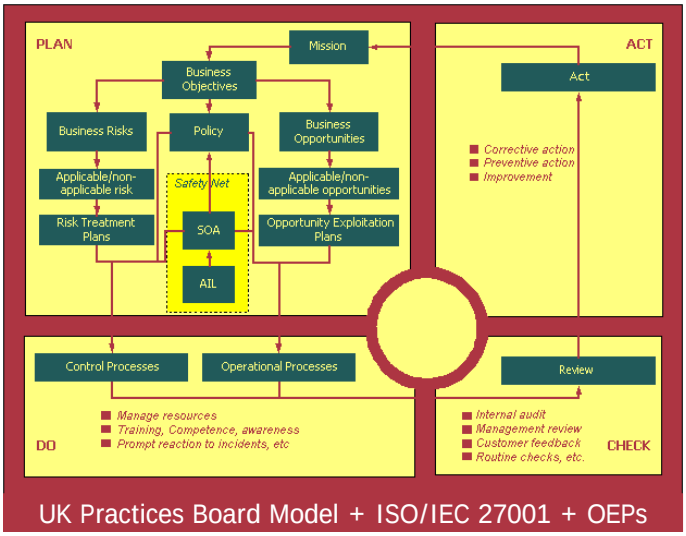




"... detect the event in sufficient time to do something positive about it..."

See http://www.gammassl.co.uk/topics/time/index.html

Internal control



UK Practices Board Model + ISO/IEC 27001 + OEPs

Summary and conclusions

- Sarbanes-Oxley and Basel II each require a sound system of internal control
- IT plays a major role, so does therefore IT security
- But it is a management issue → need a management system
- ISO/IEC 27001 is key – already part of Mauritius becoming a Cyber Island of Quality
- But it needs augmentation
  - *Sarbanes-Oxley → traceability of financial transactions*
  - *Basel II → need to measure effectiveness of controls (operational risk)*
- Unified model of internal control
- All doable

Information Security Compliance for Sarbanes-Oxley and Basel II

Computer Security Week 30th November 2006

Any Questions?

Certificate No. IS 85916

Certificate No. FS 30710

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