
Information Security Compliance for Sarbanes- Oxley and Basel II



Computer Security Week 30th November 2006



Certificate No. IS 85916



Certificate No. FS 30710

Dr. David Brewer

Gamma Secure Systems Limited

www.gammassl.co.uk

©Gamma Secure Systems Limited, 2006

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

©Gamma Secure Systems Limited, 2006

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.*

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

©Gamma Secure Systems Limited, 2006

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?

©Gamma Secure Systems Limited, 2006

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?

©Gamma Secure Systems Limited, 2006

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”

©Gamma Secure Systems Limited, 2006

ISO/IEC 27001

Information Security Management Systems - Requirements



International take-up



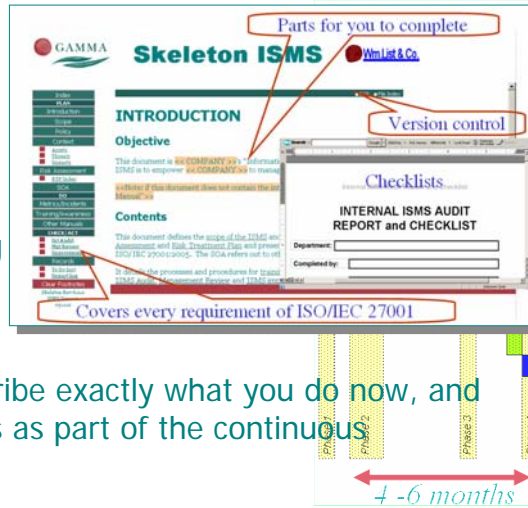
5 November 2006

■ 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



©Gamma Secure Systems Limited, 2006

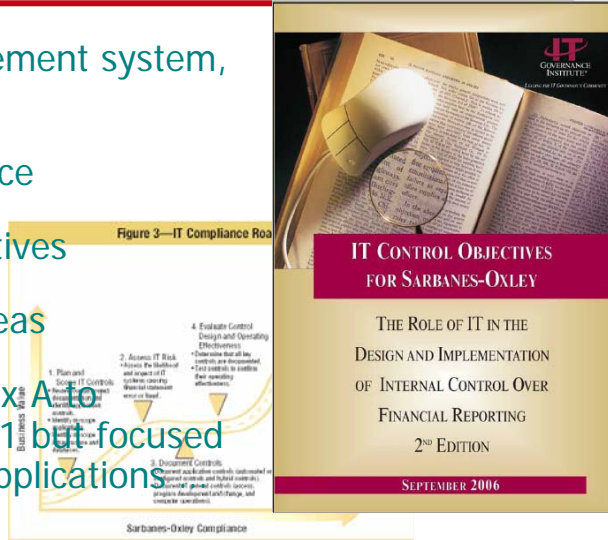
Compliance

- 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*

©Gamma Secure Systems Limited, 2006

SOX – ITGI’s CobIT

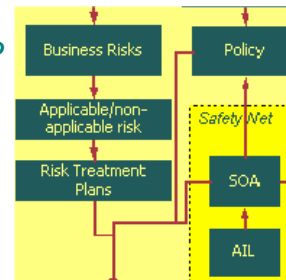
- Not a management system, but...
- Useful guidance
- Control objectives
- Alternative ideas
- Just like Annex A to ISO/IEC 27001 but focused on financial applications



©Gamma Secure Systems Limited, 2006

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



©Gamma Secure Systems Limited, 2006

Basel II

■ Credit, Market and Operational Risk

CREDIT RISK		
Primary Risk Category	Definition: the risk of loss arising from ...	Associated Operational Risk: the inadequacy or failure of internal processes, people and systems that results in a risk of ...
Project risk	... default by a creditor (which will result in a customer)	... doing work and not making a profit. 1
Trading risk	... changes in trading positions when prices move adversely.	... our money and other assets not being worth as much as they ought. 2
Market risk	... the market refusing to buy what we have to offer at the price we wish to sell it. 3	... being unable to sell what the market wants. 3
Existence risk	... the fact that we exist. 5	... spending money unnecessarily. 4

OPERATIONAL RISK		
Primary Risk Category	Definition: the risk of loss arising from ...	Associated Operational Risk: the inadequacy or failure of internal processes, people and systems that results in a risk of ...
IT risk	... company's IT is ineffective in the use to carry out the contracted work.	... if the IT isn't up to the job, or the business applications do not work as they should, the work will take longer than it ought, representing poor value for money to the customer. However, it is not judged as being significant, given the current policy for replacing and upgrading the company's IT every two years, and that special purchases when necessary.
Product risk	... we are unable to deliver our product on time.	... if not being delivered on time and potentially significant, such increased cost and time.

RISKS CONCERNING NON-APPLICABLE RISKS

It is possible that a non-applicable risk becomes an applicable risk.

All assets could be affected, but primarily Asset Group 12...

RISKS CONCERNING IT FAILURE

Gamma is reliant on its IT. The technology could fail for a wide variety of reasons, as in a wide variety of causes. Broadly speaking, the failure will result in unavailability, loss of integrity and/or loss of confidentiality. Note that integrity also implies that information is sufficiently right for the purpose for which it is used as the case that it is used, and not just that data has been modified without authorization or error. All IT based assets could be affected (Groups 2, 7, 1, 1, 1, 1).

The impacts of such events are:

- Possible inability to carry out some or all of Gamma's business, see 2.4.4, 2.4.5, 2.4.6, 2.4.7, 2.4.8
- Possible unacceptable disclosure of information, see 2.4.9, 2.4.10, 2.4.11, 2.4.12, 2.4.13, 2.4.14, 2.4.15, 2.4.16, 2.4.17, 2.4.18, 2.4.19, 2.4.20, 2.4.21, 2.4.22, 2.4.23, 2.4.24, 2.4.25, 2.4.26, 2.4.27, 2.4.28, 2.4.29, 2.4.30, 2.4.31, 2.4.32, 2.4.33, 2.4.34, 2.4.35, 2.4.36, 2.4.37, 2.4.38, 2.4.39, 2.4.40, 2.4.41, 2.4.42, 2.4.43, 2.4.44, 2.4.45, 2.4.46, 2.4.47, 2.4.48, 2.4.49, 2.4.50, 2.4.51, 2.4.52, 2.4.53, 2.4.54, 2.4.55, 2.4.56, 2.4.57, 2.4.58, 2.4.59, 2.4.60, 2.4.61, 2.4.62, 2.4.63, 2.4.64, 2.4.65, 2.4.66, 2.4.67, 2.4.68, 2.4.69, 2.4.70, 2.4.71, 2.4.72, 2.4.73, 2.4.74, 2.4.75, 2.4.76, 2.4.77, 2.4.78, 2.4.79, 2.4.80, 2.4.81, 2.4.82, 2.4.83, 2.4.84, 2.4.85, 2.4.86, 2.4.87, 2.4.88, 2.4.89, 2.4.90, 2.4.91, 2.4.92, 2.4.93, 2.4.94, 2.4.95, 2.4.96, 2.4.97, 2.4.98, 2.4.99, 2.4.100

The principal threats are hacking, failures, errors, utility failures, software failures and viruses.

©Gamma Secure Systems Limited, 2006

Basel II

■ Credit, Market and Operational Risk

CREDIT RISK		
Primary Risk Category	Definition: the risk of loss arising from ...	Associated Operational Risk: the inadequacy or failure of internal processes, people and systems that results in a risk of ...
Project risk	... default by a creditor (which will result in a customer)	... doing work and not making a profit. 1
Trading risk	... changes in trading positions when prices move adversely.	... our money and other assets not being worth as much as they ought. 2
Market risk	... the market refusing to buy what we have to offer at the price we wish to sell it. 3	... being unable to sell what the market wants. 3
Existence risk	... the fact that we exist. 5	... spending money unnecessarily. 4

OPERATIONAL RISK		
Primary Risk Category	Definition: the risk of loss arising from ...	Associated Operational Risk: the inadequacy or failure of internal processes, people and systems that results in a risk of ...
IT risk	... company's IT is ineffective in the use to carry out the contracted work.	... if the IT isn't up to the job, or the business applications do not work as they should, the work will take longer than it ought, representing poor value for money to the customer. However, it is not judged as being significant, given the current policy for replacing and upgrading the company's IT every two years, and that special purchases when necessary.
Product risk	... we are unable to deliver our product on time.	... if not being delivered on time and potentially significant, such increased cost and time.

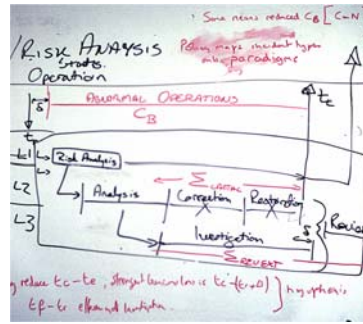
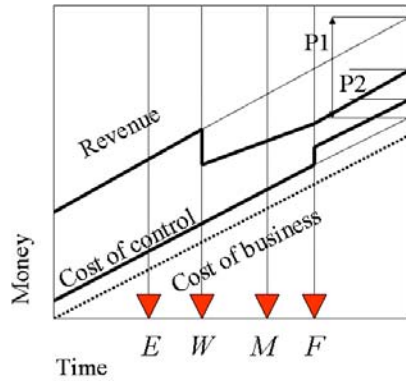
The creditor defaults

1. Invoice not raised
2. Work outside contract
3. Unacceptable quality
4. Overheads too high
5. Unable to complete the job

10. Delivery too late

©Gamma Secure Systems Limited, 2006

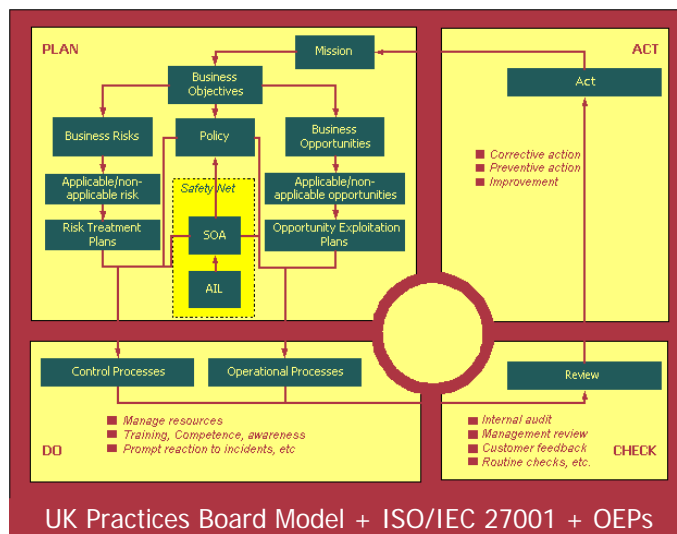
Measuring effectiveness



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

See <http://www.gammasi.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
 - *Sarbanes-Oxley* → traceability of financial transactions
 - *Basel II* → need to measure effectiveness of controls (operational risk)
- 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
- Unified model of internal control
- All doable

©Gamma Secure Systems Limited, 2006

Information Security Compliance for Sarbanes-Oxley and Basel II

Computer Security Week 30th November 2006

Any Questions?



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

©Gamma Secure Systems Limited, 2006