ISO/IEC 27001: Mapping to Operational Risk under Basel II

Dr. David Brewer, FBCS, MI OD

Conference of IT Heads of Banks, RBI, CAB, Pune 22 September 2007
Agenda

- Basel II
- A taxonomy of risk
- Measuring effectiveness
- Internal control
- Summary and conclusions

Basel Committee on Banking Supervision

International Convergence of Capital Measurement and Capital Standards

A Revised Framework

Comprehensive Version

This document is a companion to the June 2004 Basel II Framework, the elements of which are included in the Basel II process. The 2004 Amendment to the Capital Accord for International Banking Operations, and the 2003 accord for the Application of Basel II to Trading Activities, and the Treatment of Secured Debt in Effects of Measurments have been introduced in this companion.

June 2004

©Gamma Secure Systems Limited, 2007
BASEL II
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?
Operational risk

- Includes legal risk
- Excludes strategic and reputational risk
- Can use:
  - Basic indicator approach
  - Standardised approach
  - Advanced measurement approaches
Basic indicator approach

- No qualifying criteria
- Bottom line 15%

\[ K_{BIA} = \left( \sum (GI_{1...n} \times \alpha) \right) / n \]
Standardised approach

- Qualifying criteria
- Eight business lines
- Possible alternative approach for retail/commercial banking
- International banks are expected to do this
- Bottom line: could be more than 15%, could be less

\[ K_{TSA} = \left\{ \sum_{\text{years } 1-3} \max \left[ \sum (G_{1-8} \times \beta_{1-8}), 0 \right] \right\} / 3 \]

<table>
<thead>
<tr>
<th>Business Lines</th>
<th>Beta Factors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corporate finance ((\beta_1))</td>
<td>18%</td>
</tr>
<tr>
<td>Trading and sales ((\beta_2))</td>
<td>18%</td>
</tr>
<tr>
<td>Retail banking ((\beta_3))</td>
<td>12%</td>
</tr>
<tr>
<td>Commercial banking ((\beta_4))</td>
<td>15%</td>
</tr>
<tr>
<td>Payment and settlement ((\beta_5))</td>
<td>18%</td>
</tr>
<tr>
<td>Agency services ((\beta_6))</td>
<td>15%</td>
</tr>
<tr>
<td>Asset management ((\beta_7))</td>
<td>12%</td>
</tr>
<tr>
<td>Retail brokerage ((\beta_8))</td>
<td>12%</td>
</tr>
</tbody>
</table>
Advanced approaches

■ You decide

■ Within various constraints...

(n) Qualitative standards

666 A bank must meet the following qualitative standards before it is permitted to use an AMA for operational risk capital:

(a) The bank must have an independent operational risk management function that is responsible for the design and implementation of the bank’s operational risk management framework. The operational risk management function is responsible for codifying firm-level policies and procedures concerning operational risk management and controls, for the design and implementation of the firm’s operational risk measurement methodology, for the design and implementation of a risk-reporting system for operational risk, and for developing strategies to identify, measure, monitor and control/mitigate operational risk.

(b) The bank’s internal operational risk measurement system must be closely integrated into the day-to-day risk management processes of the bank. Its output must be an integral part of the process of monitoring and controlling the bank’s operational risk profile. For instance, this information must play a prominent role in risk reporting, management reporting, internal capital allocation, and risk analysis. The bank must have techniques for allocating operational risk capital to major business lines and for creating incentives to improve the management of operational risk throughout the firm.

(c) There must be regular reporting of operational risk exposures and loss experience to business unit management, senior management, and to the board of directors. The bank must have procedures for taking appropriate action according to the information within the management reports.

(d) The bank’s operational risk management system must be well documented. The bank must have a routine in place for ensuring compliance with a documented set of internal policies, controls, and procedures concerning the operational risk management system, which must include policies for the treatment of non-
Qualifying criteria

Both standardised and advanced approaches require a sound system of internal control with director/senior management oversight (as a minimum)

660. In order to qualify for use of the Standardised Approach, a bank must satisfy its supervisor that, at a minimum:

- Its board of directors and senior management, as appropriate, are actively involved in the oversight of the operational risk management framework;
- It has an operational risk management system that is conceptually sound and is implemented with integrity, and
- It has sufficient resources in the use of the approach in the major business lines as well as the control and audit areas.

661. Supervisors will have the right to insist on a period of initial monitoring of a bank’s Standardised Approach before it is used for regulatory capital purposes.

662. A bank must develop specific policies and have documented criteria for mapping gross income for current business lines and activities into the standardised framework. The criteria must be reviewed and adjusted for new or changing business activities as appropriate. The principles for business line mapping are set out in Annex 8.
Basel intentions

- Sound, measurable internal control
- Director/senior management participation
- Documentation, records
- Continual improvement
- Systematic, well argued approach backed by real data
Mapping to ISO/IEC 27001

- ISO/IEC 27001 requires:
  - Director/senior management oversight
  - Sound risk management framework
  - Documentation
  - Measurements
  - Repeatable/reproducible results
  - Feedback, both internal and external

- Not a bad match…

- Information security is part of operational risk
A TAXONOMY OF RISK
A taxonomy of risk

Credit, Market and Operational Risk

**CREDIT RISK**

- Project risk: default by a creditor (which will usually be a customer).
- Trading risk: changes in trading positions when prices move adversely.
- Market risk: the market refusing to buy what we have to offer at the price we wish to sell it.
- Existence risk: the fact that we exist.

**MARKET RISK**

- Project risk: default by a creditor (which will usually be a customer).
- Trading risk: changes in trading positions when prices move adversely.
- Market risk: the market refusing to buy what we have to offer at the price we wish to sell it.
- Existence risk: the fact that we exist.

**OPERATIONAL RISK**

- 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 usually be a customer).
- Trading risk: changes in trading positions when prices move adversely.
- Market risk: the market refusing to buy what we have to offer at the price we wish to sell it.

**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 E.

**RISKS CONCERNING IT FAILURE**

Gamma is reliant on its IT. The technology could fail for a wide variety of reasons and in a wide variety of manners. Broadly speaking, the failure will result in unavailability, loss of integrity and/or loss of confidentiality. Note that the integrity also relates to information sufficiently rich for the purpose for which it is used at the time it is used, and not just that data has been modified without authorization or error. All IT based assets could be affected (Group E, E, E, E, E).

The impacts of such events are:
- Possible inability to carry out any or all of Gamma’s business, see 5.4.1a.
- Security data disclosure (see 5.3.1)
- Possible unauthorized disclosure of sensitive data (see 5.1.2a)

The principal threats are backup failure, errors, utility failure, software failure and viruses.

©Gamma Secure Systems Limited, 2007
A taxonomy of risk

Credit, Market and Operational Risk

**CREDIT RISK**
- Definition: the risk of loss arising from...
- Project risk: default by a creditor (which will usually be a customer).
- Trading risk: changes in trading positions when prices move adversely.
- Existence risk: the fact that we exist.

**MARKET RISK**
- Definition: the market refusing to buy what we have to offer at the price we wish to sell it.
- Market risk: our money and other assets not being worth as much as they ought.
- Delivery too late.

**OPERATIONAL RISK**
- Definition: the inadequacy or failure of internal processes, people and systems that results in a risk of...
- Operational risk: doing work and not making a profit.
- Unacceptable quality.
- Overheads too high.
- Unable to complete the job.

1. Invoice not raised
2. Work outside contract
3. Unacceptable quality
4. Overheads too high
5. Unable to complete the job
6. The creditor defaults
7. Being unable to sell what the market wants.
8. Storage of company's IT is ineffective in allowing us to carry out the contracted work.
9. 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 is worth compensating.
10. Delivery too late

©Gamma Secure Systems Limited, 2007
Operational risk - 1

- Invoice not raised:
  - How do you ensure all invoices that should be raised are issued, and issued correctly?

- IT solutions:
  - Substantive audit
  - Correctness of billing system
  - Customer authentication
  - ...

- Integrity

- Failure of internal control in respect of CREDIT risk
Operational risk - 2

- Mark to market:
  - *How do you ensure the valuation of futures are in accordance with the rules?*

- IT solutions:
  - *Automated test programs to detect:*
    - Correspondence to reality
    - Database anomalies
    - Rate curve is valid
    - Valuation by trade

- Integrity

- Failure of internal control in respect of MARKET risk
Customer details leaked:

- How do you ensure customer data is not given to unauthorised people?

IT solutions:

- Caller authentication
- Access control
- Website design
- Firewalls

Confidentiality (Data Protection Act)

General OPERATIONAL risk
Operational risk - 4

- Operator error:
  - What do you do if someone makes a mistake?

- IT solutions:
  - Access control
  - Check and release
  - Back-up
  - Audit
  - ...

- Integrity

- General OPERATIONAL risk
Operational risk - 5

- Disaster:
  - What do you do if the computer breaks? (part of business continuity)

- IT solutions:
  - Back-up
  - Hot, warm standby
  - Disaster recovery site
  - …

- Availability
- General OPERATIONAL risk
Computers play a major role

All sorts of things can go wrong

Information security is a significant component of operational risk

ISO/IEC 27001 addresses this:

- Risk assessment/risk treatment
- Incident handling
- A comprehensive set of 133 controls
MEASURING EFFECTIVENESS
The “Time” model
Event-impact relationship

There is a fundamental principle of internal control (and thus ISMS):

“… detect the event in sufficient time to do something positive about it… “

See http://www.gammassl.co.uk/topics/time/index.html
Fundamental model (too late)
Fundamental model (in time)
Control spectrum

<table>
<thead>
<tr>
<th>Class</th>
<th>Ability to detect the event and take recovery action</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Prevents the event, or detects the event as it happens and prevents it from having any impact</td>
<td>Preventive</td>
</tr>
<tr>
<td>2</td>
<td>Detects the event and reacts fast enough to fix it well within the time window</td>
<td>Detective</td>
</tr>
<tr>
<td>3</td>
<td>Detects the event and just reacts fast enough to fix it within the time window</td>
<td>Preventive</td>
</tr>
<tr>
<td>4</td>
<td>Detects the event but cannot react fast enough to fix it within the time window</td>
<td>Preventive</td>
</tr>
<tr>
<td>5</td>
<td>Fails to detect the event but has a partially deployed BCP</td>
<td>Reactive</td>
</tr>
<tr>
<td>6</td>
<td>Fails to detect the event but does have a BCP</td>
<td>Reactive</td>
</tr>
<tr>
<td>7</td>
<td>Fails to detect the event and does not have a BCP</td>
<td>Reactive</td>
</tr>
</tbody>
</table>
Effectiveness

Theory and Practice
Mapping to ISO/IEC 27001

ISO/IEC 27001 requires measurement of the effectiveness of controls

This is one way to do it (and probably the best)

In addition to the time parameters:

- We consider the impact that training has on the number of incidents, the metric being of the form the number of incidents that could have been prevented by better training divided by the total number of incidents.
- Similarly we consider the impact that training has on the number of nonconformities discovered by internal ISMS audit, the metric being of the form the number of nonconformities that could have been prevented by better training divided by the total number of nonconformities.

Add to this list any other metrics you wish to use

<<<>
Event – driven Risk Treatment plans

Risk Treatment Plans

In this section we propose a methodology for generating Risk Treatment Plans, which makes use of the fundamental theory which we have just discussed.

We have used the methodology extensively in the information security arena. We have taught senior managers/risk owners how to use it in various parts of the world and they have been able to apply it, not only in the context of information security but also to other business/governance concerns. We therefore believe that this methodology works and is repeatable, reproducible and robust.

We start by saying a little more about events and impacts on which the methodology is founded.

Events

The events referred to in this paper are bad things that cause trouble. The insert (right) lists those events, which in our R5/55 work we believe are common across many businesses. In addition we would add other events that were specific to that particular organisation. An example would be one of our aircraft has broken down.

Events that are likely to be common across many businesses are:

- Theft
- Acts of God, vandals and terrorists
- Regular fraud
- Industrial action

©Gamma Secure Systems Limited, 2007
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

Treat the risk

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

Select the controls

Choose the appropriate controls
Tell it like a story

- Predicated on “Time Model”
- Repeats the question “what if it doesn’t work”
- Expressed in business terms in language everyone can understand
Options for treating risk

- Avoid the risk
- Accept the risk
- Transfer the risk
- Mitigate the risk
**Overview**

### Data Table

<table>
<thead>
<tr>
<th>Asset ID</th>
<th>Description</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Threat Agent ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Vulnerability ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Impact ID</th>
<th>Description</th>
<th>Magnitude</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Description</th>
<th>Circumstance</th>
<th>Likelihood (or frequency)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

**Risk Mitigation Criteria**

- State your risk mitigation criteria.
- Describe the action that is taken if a risk is found to be unacceptable.

**Instructions for Dealing with Unacceptable Risk**

> An example, a report may need to be written and submitted to management for approval; the proposed plan may need to identify recommended action, measures, and related consideration of the event's circumstances and responsibilities, etc. It might also give an indication of what the residual risk would be.

**Risk Treatment Plans (RTPs)**

Each RTP presents the overall design of a suite of controls that will prevent an event, or that cannot be done or a control fails, how to handle something about it, and if that fails how to mitigate and/or recover. We make use of the Brewer-Lee time theory referred to above, where we anticipate of events (i.e., the use of tell-tale signs, based on previous events). There is one RTP for each event:

- List each event and link it to the relevant RTP page.

**Summary of Residual Risk**

Summarise here the residual risks. Use a table, or perhaps a picture. Highlighting will help. There will be having followed the instructions cited above on dealing with...
An example

E3.1 Precautions

We take precautions against fire, flood, [...] and theft for all physical information containers, whether within our scope of control, outside of it (whilst traveling and working away form the office on a temporary or extended basis) or in transit (in person or by courier or post). We know what our assets are, where they are and who is responsible for them. We require our employees and contractors to return them when requested to do so. Nevertheless it is still possible that such containers may be damaged or destroyed by fire, flood, [...], stolen, lost or misappropriated (e.g. lost in the post). Containers may also be deliberately discarded or reused by someone who is not permitted to see the original contents.

E3.2 Detection in general

Fire, other damage, theft and loss is usually obvious. [Add steps to detect events if felt not some obvious] As our employees and contractors are not permitted to put themselves in danger, however, it is accepted that the detection of these events whilst they are in progress will normally not allow the impacts to be prevented.

E3.3 Detection of loss in transit

[say how loss of containers in transit by post, courier are detected]. Disposal is, of course, a deliberate action. Not to know that a container has been dispossessed is therefore an acceptable risk.

E3.4 Insurance

The loss of the monetary value of dispossessed assets is an insurance risk. [elaborate as appropriate] The risk
Typical IS events and impacts

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

Covers all 133 controls

©Gamma Secure Systems Limited, 2007
Basel II required events

- Internal fraud
- External fraud
- Employment Practices and Workplace Safety
- Clients, Products & Business Practices
- Damage to Physical Assets
- Business disruption and system failures
- Execution, Delivery & Process Management
Mapping to ISO/IEC 27001

- ISO/IEC 27001 requires an assessment to be performed but does not specify how to do it

- The Brewer-List methodology is appropriate

- Basel II specifies certain event loss types

- Use these to design the Risk Treatment Plans

- Supplement with other RTPs to deal with other operational risks

- Note that insurance is recognised by ISO/IEC 27001 as a particular mode of risk treatment
Effectiveness Measurement

Measuring Effectiveness

In cases where there has been an incident, a near miss or a nonconformity concerning information security controls, we determine the values of the various time parameters:

- $T_e$: the time that the event occurred
- $T_d$: the time that the event was detected by the control, or if there was control, the time the control failed, the time $T_e$ at which management noticed the problem or it was otherwise brought to their attention
- $T_r$: the time at which the problem was corrected
- $T_i$: the time at which the impact occurred

©Gamma Secure Systems Limited, 2007
A method

- Q1 - Did the controls work as designed?
- Q2 - If they did, should they be improved?
- Q3 - in either case, is there a training issue?
- Q4 - is there a process issue?
- Q5 - is there a technical issue?
- Q6 - is there a RTP design issue?
Mapping to ISO/IEC 27001

- ISO/IEC 27001 requires the measurement to be done but does not specify how to do it.

- The time theory provides the basis of such a method.

- Tailor it to your bank’s specific ways of doing things and the Basel II requirements (for AMA).
Corporate governance

- A result of scandals ... investing public ... being "ripped off" ... conduct of senior executives
  - South Sea Bubble, Kruger, Salad Oil company, Equity Funding, Polly Peck, Maxwell Pensions, Enron, WorldCom ...
- New laws/regulations ... anti discrimination, privacy protection, product quality, environment etc.
- Turnbull, OECD, Sarbanes-Oxley, EU directive
Internal control

A WORD OF WARNING

In US Only financial reporting

In UK Everything

In INDIA Rule 49 Financial reporting + risk management

Definitions differ around the world!

©Gamma Secure Systems Limited, 2007
Research conclusions

- A conclusion of the Time paper was that (ISO) standards are just aspects of internal control.

- Further research identified the need for a PDCA engine to drive the system of internal control.
A model of internal control

UK Practices Board Model + ISO/IEC 27001 + OEPs
Opportunity exploitation plans

The converse of events and impacts

We have a range of products, some established (of which some will have just been improved), new products and the results of our own R&D projects. The Market Presence Opportunity prepares the way for selling our products by generating market presence.

Similar “time” theory

But not required for Basel II (because failure to exploit an opportunity is primarily a strategic risk)

Anticipated benefits

Reaping the benefit

Loosing the opportunity

Secure Matrix

©Gamma Secure Systems Limited, 2007
Mapping to ISO/IEC 27001

- ISO/IEC 27001 meets all the requirements of the PDCA engine necessary to drive a system of internal control.

- OEPs are not part of ISO/IEC 27001 or Basel II but can be used to justify risk exclusions.

- But could give a bank a considerable edge against larger international competitors.
SUMMARY AND CONCLUSIONS
Summary and conclusions

- Basel II extends credit/market risk to operational risk
- For SA and AMA, Basel II requires a sound system of internal controls, with senior management participation
- For AMA, Basel II places constraints on measurements of effectiveness and event loss types
- IT security is a significant component of operational risk
- ISO/IEC 27001 addresses this and provides the necessary PDCA framework
- We have a method for dealing with the other Basel II operational risk requirements
- There is an opportunity for exploiting the Basel II regulations
ISO/IEC 27001: Mapping to Operational Risk under Basel II

Any Questions?

Dr. David Brewer, FBCS, MIOD

dbrewer@gammassl.co.uk
www.gammassl.co.uk