
# The IT Security Implications of Basle II

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


*Certificate No. IS 85916*


*Certificate No. FS 30710*

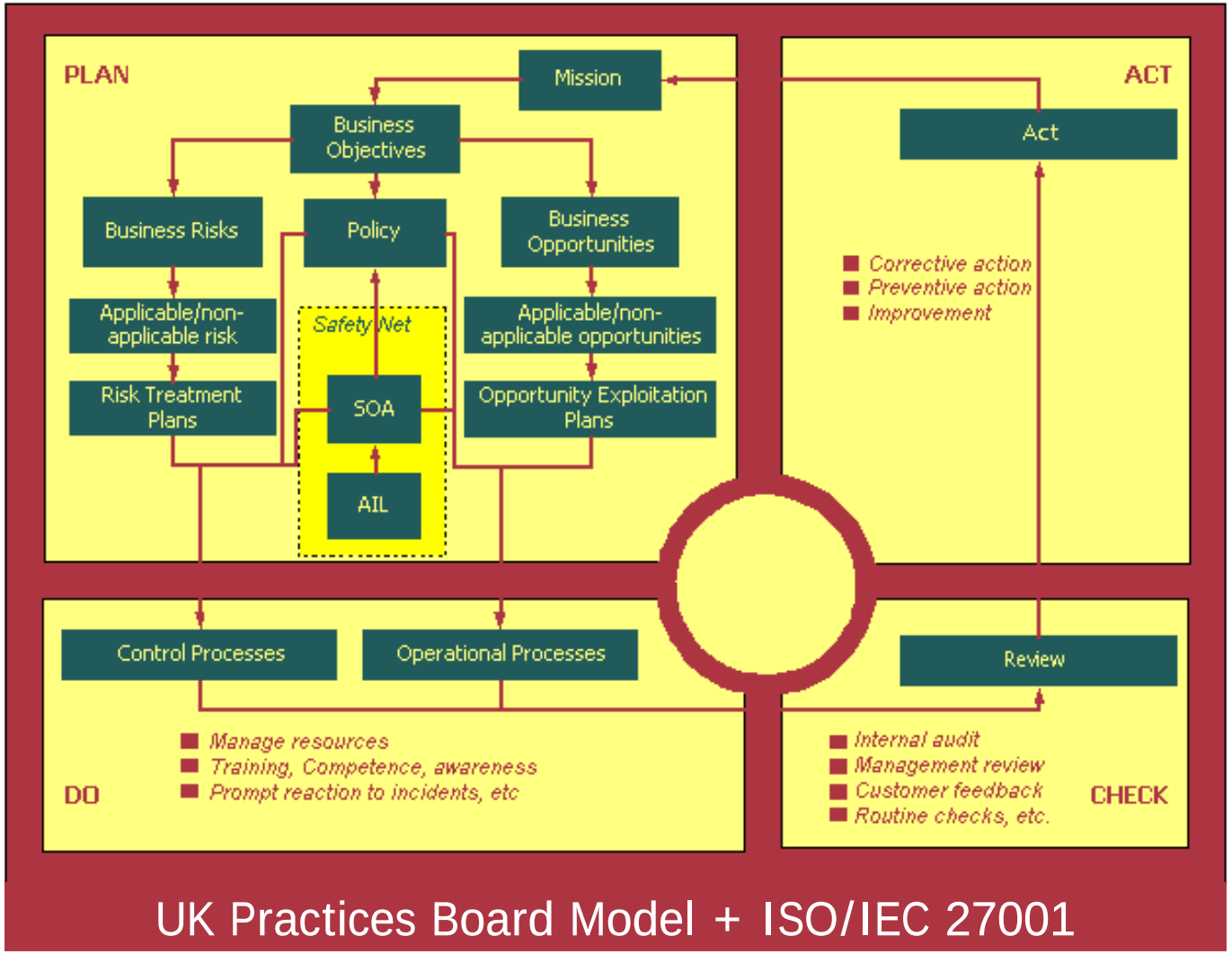
# Agenda

- Basle II
- Internal Control
- IT Security
- Taxonomy of Risk
- Risk Treatment
- Operational Risk
- Effectiveness
- Summary and Conclusions

# Basle II

- Extends credit/market risk provisions of Basle 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?

# Internal Control




UK Practices Board Model + ISO/IEC 27001

# IT Security

- Log-on, encryption, anti-virus, access control, firewalls ...
- Preventive measures
- What if it doesn't work:
  - *Need to detect event in sufficient time to prevent/mitigate the impact*
- Confidentiality, integrity, availability
- Standards: technical, evaluation, management

# Taxonomy of 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 usually be 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. | ... being unable to sell what the market wants. 3 |
| Existence risk | ... the fact that we exist. 5 | ... spending money unnecessarily. 4 |

**MARKET RISK**

**OPERATIONAL RISK**

# Taxonomy of 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 usually be a customer). | ... doing work and not making a profit. |
| Market risk | ... the market re... what we have to ... price we wish to ... | |
| Existence risk | ... the fact that w... | |

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

**IT? Depends on role played by IT**

# Risk Treatment

- Basle defines formulae for credit/market risk
- IT uses formulae (R = T * A * V), but this is impractical (and only assesses risk)
- "Tell it like a story" works better

Then the adjusted value of the collateral, $C_A$, is

$$C_A = \frac{C}{1 + H_E + H_C + H_{FX}}$$

$$= \$1{,}000/(1+0.04+0+0)$$

$$= \$962.$$

In order to calculate the risk weighted assets, risks ($w$=0.15), and the risk weight of counte below. Note that the exposure ($1,000) exceed

$$r^* x E = r x [E - (1-w) x C_A]$$

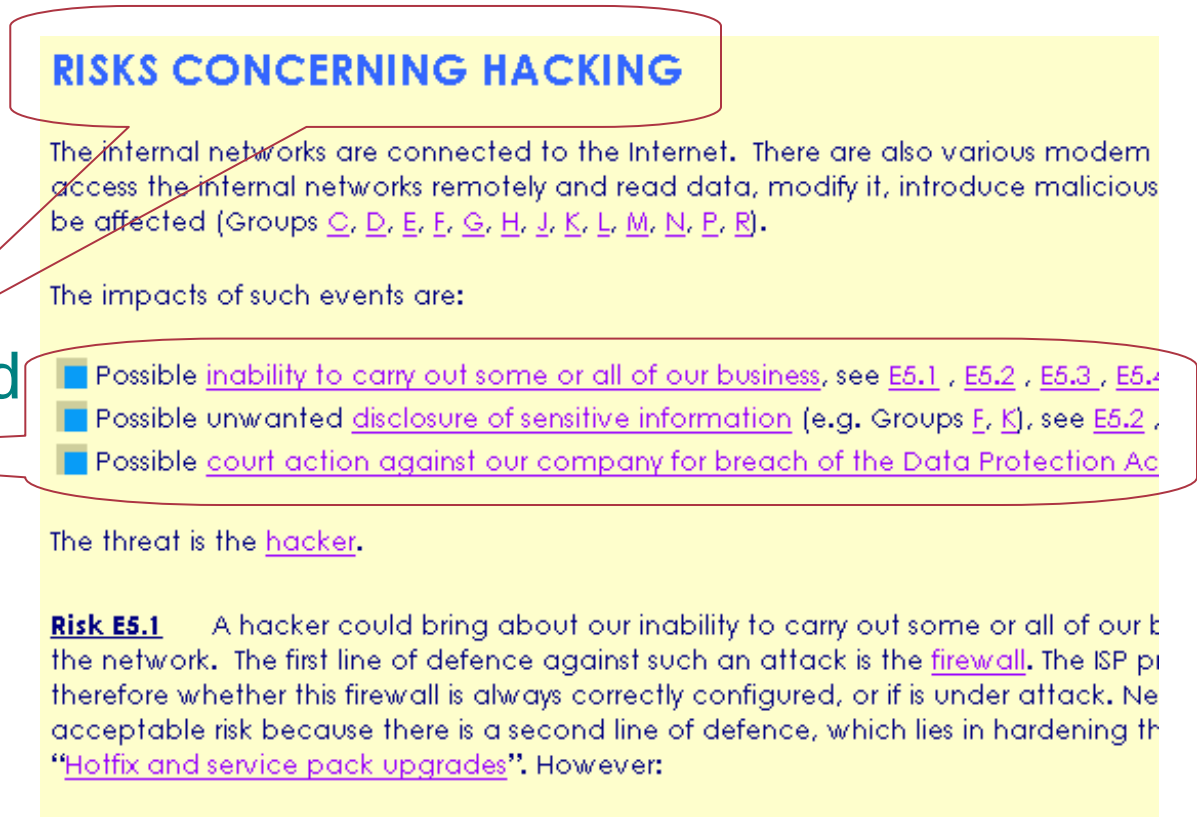
$$r^* \times 1{,}000 = 0.2\,[1000 - (1-0.15) \times 962$$

$$r^* = 3.65\%$$

and so the risk weighted assets will be $36.50.

# Risk Treatment

- Performed by risk owners – the Board
- Tell it like a story
- Business events and impacts
- Public methodology
  - *Good plot*
  - *Happy ending*



**RISKS CONCERNING HACKING**

The internal networks are connected to the Internet. There are also various modem access the internal networks remotely and read data, modify it, introduce malicious be affected (Groups C, D, E, F, G, H, J, K, L, M, N, P, R).

The impacts of such events are:

- Possible inability to carry out some or all of our business, see E5.1 , E5.2 , E5.3 , E5.
- Possible unwanted disclosure of sensitive information (e.g. Groups F, K), see E5.2 ,
- Possible court action against our company for breach of the Data Protection Ac

The threat is the hacker.

**Risk E5.1** A hacker could bring about our inability to carry out some or all of our b the network. The first line of defence against such an attack is the firewall. The ISP p therefore whether this firewall is always correctly configured, or if is under attack. Ne acceptable risk because there is a second line of defence, which lies in hardening th "Hotfix and service pack upgrades". However:

# 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

# Operational Risk - 3

- 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*
  - *…*

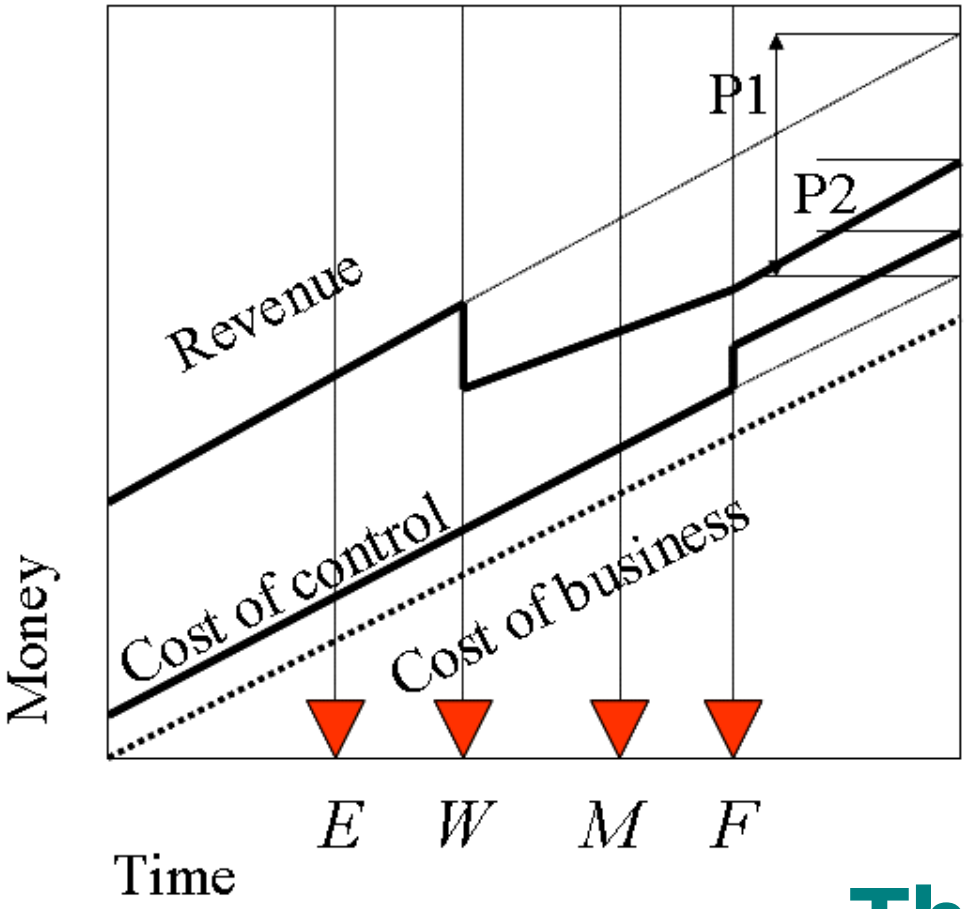
- Availability
- General OPERATIONAL risk

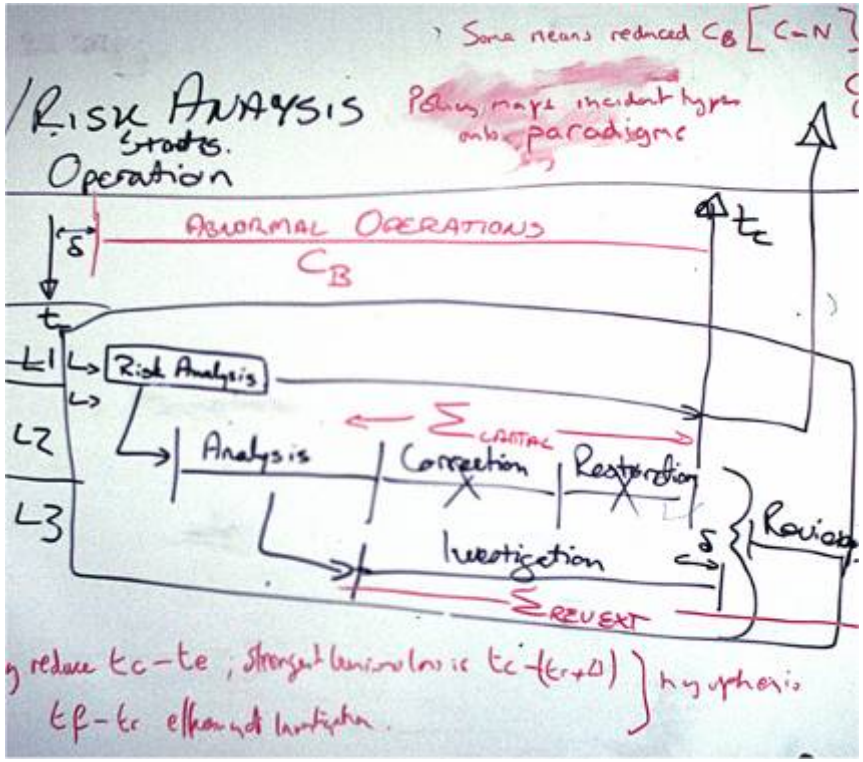
# Effectiveness

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

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

# Effectiveness




## Theory and Practice

# Summary and Conclusions

- Basle II extends credit/market risk to operational risk
- Operational risk can be subdivided
- Need to measure effectiveness
  - *Overall Plan-Do-Check-Act framework*
  - *Time metrics*
  - *Tell it like a story Risk Treatment Plans*
- IT plays a major role, so does therefore IT security
- All part of internal control
- All doable

GAMMA

# The IT Security Implications of Basle II

*Any Questions?*

Certificate No. IS 85916

Certificate No. FS 30710