



Programme on Designing Information Systems for Business & Basel II

June 18 – 21, 2007

IT Risk Management for Basel II

V G Sekar
DGM & Member of Faculty
CAB, RBI

Date:

College of Agricultural Banking, RBI, PUNE



Operational Risk: An intro

- *Basel II definition of Operational Risk: Risk of loss resulting from inadequate or failed internal processes, people and systems or from external events.*
- The definition includes legal risk, but excludes strategic and reputational risk.
- To assess the amount of operational risks, the banks may use various alternative approaches: BIA, STA & AMA



Operational Risk Management Framework



Date:

College of Agricultural Banking, RBI, PUNE



IT-related Risks Identified by Basel II

**I
T
R
I
S
K
S**

Potential to transform risks from manual processing errors to system failure risks

Growth of e-commerce brings with it potential risks

Viability issues of new or newly integrated systems

Need for continual maintenance of high-grade internal controls and back-up systems

Date:

College of Agricultural Banking, RBI, PUNE



Operational Risk Events

Basel II Type Events	IT Aspects
Internal fraud	<ul style="list-style-type: none">▪ Deliberate manipulation of programs▪ Unauthorized usage of modification functions▪ Deliberate manipulation of system instructions▪ Deliberate manipulation of hardware▪ Deliberate changing of system and application data through hacking▪ Using/copying unlicensed or unauthorized software▪ Internal circumvention of access privileges
External fraud	<ul style="list-style-type: none">▪ Deliberate changing of system and application data through hacking▪ Outsiders gaining sight of confidential physical or electronic documents▪ External circumvention of access privileges▪ Eavesdropping and interception of communication links▪ Password compromise▪ Viruses
Employment practices and workplace safety	<ul style="list-style-type: none">▪ Misuse of IT resources▪ Lack of security responsiveness

Date:



Operational Risk Events...

Clients, products and business practices	<ul style="list-style-type: none">▪ Disclosure of sensitive information to outsiders by employees▪ Management of third-party suppliers
Damage to physical assets	<ul style="list-style-type: none">▪ Deliberate or accidental damage to physical IT infrastructure
Business disruption and system failures	<ul style="list-style-type: none">▪ Hardware or software malfunction▪ Communications failure▪ Employee sabotage▪ Loss of key IT staff▪ Destruction of software/data files▪ Theft of software or sensitive information▪ Computer viruses▪ Failure to back up▪ (Distributed) denial-of-service attacks▪ Configuration control error
Execution, delivery and process management	<ul style="list-style-type: none">▪ Error in handling electronic media▪ Unattended workstation▪ Change control error▪ Incomplete input of transactions▪ Errors on data input/output▪ Programming/testing error▪ Operator error, e.g., in recovery procedural error

Date:



Guiding Principles for IT Risk Management under Basel II

There is a need for an operational risk mgt framework.	IT is a critical component of operational risk.
The operational risk management framework is subject to effective and comprehensive internal audit.	The internal IT audit function should be adequately skilled and staffed in line with the IT risk profile.
Develop policies, processes and procedures for managing operational risk.	IT should use GRC frameworks (e.g., COSO) to integrate IT-specific risk within the overall corporate risk mgmt process.
Identify and assess operational risk.	IT risk assessment results should be integrated with other risk assessments and incorporated into the GRC framework.
Regularly monitor operational risk profiles and material exposure to losses.	IT should identify acceptable limits of risk and develop metrics to measure performance against these profiles.



Guiding Principles for IT Risk Management under Basel II...

Have policies, processes and procedures to control and/or mitigate material operational risks.	IT risk policy and subsidiary procedures.
Have contingency and business continuity plans.	IT continuity plans and incident response management.
Conduct regular independent evaluation of a bank's policies, procedures and practices related to operational risk.	IT should document the IT risk profile for the supervisory review process & external audit of IT-related risk management.
Provide sufficient public disclosure.	IT should identify all relevant risks that constitute a material operational risk in the sense of disclosure as defined by senior management, escalate where necessary to appropriate stakeholders and take corrective action.



Acknowledgements & Further References

- www.bis.org
- www.isaca.org
- www.coso.org
- www.kriex.org



THANK YOU



Date:

College of Agricultural Banking, RBI, PUNE