RBI's
GOPALAKRISHNA WORKING GROUP

V. Rajendran

http://venkrajen.in

venkrajen@yahoo.com

044-22473849; 9444073849

Certain concepts

- RBI's role as the Nation's Financial Regulator
- Supervising and monitoring mechanism
- Advent of Technology in banks
- Committees on Technology like
  - Jilani Working Group 1995 EDP Audit
  - Narasimhan Committee on IS Audit
  - Vasudevan Committee
  - Dr. RD Burman Working Group
- Vision Document, IT Policy Document etc
- Now GG Working Group

Gopalakrishna Working Group

- Monetary Policy Statement of April 2010, recommending enhancing RBI guidelines on IT governance, Info Sec measures to tackle cyber fraud, enhance IT controls
- Objective was to provide a set of guidelines to banks covering the entire gamut of electronic banking.
- To serve as a common minimum standard for all banks, to adopt and lay down the best practices for banks to adopt in a phased manner for a safer and sounder banking environment.
- Need for banks to follow a consistent approach in each focus area, to minimize differing interpretations

GG WG Report

- The Group examined various issues on IT
- Recommendations in nine broad areas namely
- IT Governance, Information Security, IS Audit, IT Operations, IT Services Outsourcing, Cyber Fraud, Business Continuity Planning, Customer Awareness programmes and Legal aspects.
- Report was submitted in January 2011
- Views/comments of all stake-holders/public invited
- Final guidelines circulated to commercial banks except RRBs vide RBI Circular dated 29 April 2011.
- Circulated to all banks in April 2011

GG - WG

- Some of the guidelines are re-iteration of earlier procedural guidelines and circulars already stated or issued by RBI
- Some are in the form of enhancement in Information Security initiatives already taken by banks, like introduction of 2-factor authentication in Internet Banking, introduction of ISMS like ISO 27001 standards etc.
- Not "one-size-fits-all" – WG remarks.

GG – WG Timelines

- Banks to ensure implementation of basic organizational framework and put in place policies and procedures not requiring extensive budgetary support, infrastructural or technology changes, by October 31, 2011.
- Other guidelines need to be implemented in one year unless a longer time-frame is indicated in the circular.
- A review of the implementation status to be put up to the Board at quarterly intervals.
- Incorporate in their Annual Report from 2011-12 onwards broadly the measures taken on the areas in the guidelines.
- RBI to review the progress in implementation guidelines on a quarterly basis and in its AFI from 2011-12 onwards.

IT Governance

- Board approved IT Policy document
- Exclusive Board level IT Strategy committee
- IT Steering Committee –Roles of CIO etc
- IT Resources utilisation, infrastructure
- Enterprise data dictionary – sharing of data
- Risk Management Policy ORM Policy to include IT related risks
- Framework like COBIT to be considered
- An IT balanced scorecard consider for implementation
- Assess IT maturity level based on international models (CMM?)

Information Security

- Board approved ISS Policy - Role of CISO (GM/DGM/.AGM)
- Risk Assessment: Threats and vulnerabilities
- Digital Evidence – Challenges to integrity
- Inventory of Information Assets
- Job Application review – KRA / Job Cards
- Alerts on the use of same machine for maker-checker
- Dissuade direct back-end updates to database
- Source Code from vendors
- Data transfer from one system to another – Straight through processing – audit trails
- Critical functions and reports – No use of spread sheets
- Commercial banks should implement ISO 27001 based ISMS

Info Security contd

- VAPT and other assessment
- 2-factor authentication, cryptography, OTP etc
- SMS alerts for critical areas, use of EV-SSL
- Consider use of chip-based cards
- PIN based authorisation at PoS
- Forum for CISOs – Role of IDRBT
- Multi disciplinary authority involving IIBF,IDRBT, DSCI etc coordinated by IBA

IT Operations

- Board to oversee IT operations
- HR, Infrastructure, technology etc
- IT Service Management
- Analyze Patterns of Business Activities
- Service Level Management process for SLAs
- Capacity Management Process
- Identify Vital Business Functions
- Functions like Event Management, Incident Management, Problem Management and Access Management

IT Outsourcing

- Vendor Managed Process
- Need to outsource 'material' – qualitative judgement by banks
- Diligence to assess the technology provider
- Banks' responsibility in the case of multi service provider environment
- Internal controls of the service provider – adequate?
- Country risk: economic, geographic etc – Assess
- Conduct audit, assess the service provider
- IBA may provide scoring information for service providers

IS Audit

- Audit committee to the Board
- Internal Controls – Review and oversee
- IS Audit Head – Chief Audit Executive
- Documented IS Audit Policy –Annual Review
- Risk Based Audit Approach –Methodology
- IS Audit Policy –Annual Review
- Focus on Large and Medium branches
- Password policy, User Management etc
- Application audit – Usage of CAATs
- Third party services within the scope of IS Audit of banks

Cyber Frauds

- Special Committee to the Board for frauds involving Rs.1 crore or more. For frauds of smaller amounts but large in number, Special Committee to be briefed
- Root cause analysis for fraud cases above Rs.10 lakhs
- Share details of employees who have defrauded like CIBIL, so that they are not employed anywhere else
- Transaction Monitoring Unit within Fraud Risk Management Group of banks
- Ambiguity on the Fraud Report to RBI – amount net of recovery or the gross amount – And when entire amount recovered?
- Cyber Crime – jurisdiction issue and police co-ordination issues

BCP

- Designate Head of BCP function
- People aspect is an integral part of BCP
- IS Auditors to test BCP effectiveness also
- BCP Drill – includes testing of staff at DRS
- Consider unplanned BCP Drill – involving a small set of people only
- Data integrity between DC and DR
- Redundancy in other areas like telecom lines
- Industry level alarm/crisis management team

Customer Education

- Identify and involve key stake-holders
- Awareness programme for customers
- Research Group with a repository of case-studies, sample mails, fraudulent documents etc
- Awareness programme for bank employees, customers, law enforcement personnel, media partners etc
- Evaluation of effects of various campaigns
- Banks' documented policy – industry level sharing of research units etc

Legal Issues

- Adequate Staffing to handle legal risks
- Operational Risk –Reputational risk due AML and associated non-compliance
- Evidentiary value of e-record – Attestation by bank official – Records from ATMs etc
- 2-factor authentication for credit card operations etc
- Encryption Committee of Central Govt
- Need for more legislations on EFT etc

Questions ???

Thank you…..

V. Rajendran

venkrajen@yahoo.com

info@venkrajen.in

044-22473849; 9444073849