AUDIT IN CBS ENVIRONMENT

CA Abhijit P. Sanzgiri

Do we know what we do not know

- Awareness of Limitations
- Understanding of Risks – Controls
- Explosion of data handled – speed of handling data – storage capacities –
- Desktops to laptops to handhelds –
- Do we know what the future has in store –
- Connectivity costs have come down significantly
- Boom in Digital Economy – payment banks Apps
- Banking will flourish – Banks may diminish -
- Information aggregation is not a challenge – Information segregation is

CBS – shift from branch to bank Banking

- Business Process Reengineering – Bank & not Branch Customer
- Allows any branch of a bank to view & update a common data base in a central server located in the data centre
- CBS application software
- Network connectivity through VPN (Internet)
- Web, application & database servers
- Decentralized data processing - centralized storage & backup
- Integrates various business channels of the bank
- Consolidated view of operations
- DRC (Disaster Recovery Centre) in a separate seismic zone

Software Packages

- **Core banking** - Banking service provided by a group of networked bank branches where customers may access their bank account & perform basic transactions from any member branch offices –
- Platform where communication technology & information technology merge to suit core needs of banking tailoring products & services for the customer in a proactive way
- ANY where Banking – Any Time Banking

- **Centralized online real time environment**

- Finacle – Infosys – ICICI / IDBI
- Flex Cube – Iflex – Yes Bank / Kotak Mahindra
- B@nks 24 – TCS – SBI Group
- Omni – Various Co-operative Banks

Management of big data

- CRM - 360 degree customer view
- Origination of new products & customers
- Banking analytics - Risk & Profitability analysis, Capital reserve allocation & collateral management
- Banking finance - General ledger & reporting
- Banking channels - Teller systems, side counter (sales) applications, mobile banking & online banking solutions
- Best practice workflow processes
- Content management facilities
- Governance & compliance capabilities - Internal controls management & auditing
- Security control & audit capabilities

Banking will remain – Banks may not

- Big data – 3 V's - Volume, Variety & velocity (speed)
- Scalability of systems – whether legacy architecture can support new technology -
- Internet of Things - Way for devices connected to Internet to communicate & share information, real time with other 'smart' devices leveraging capabilities of big data, analytics & artificial intelligence to anticipate needs, solve problems & improve efficiency by offering advice, products & solutions helping customers make smart & financially sound decisions
- *Cloud computing* - A type of Internet-based computing where servers, storage and applications are delivered to an organization's computers & devices through the Internet.

SA 315 -

- Identifying & assessing risk of material mis-statement through understanding of an entity & its environment –

- Obtaining sufficient understanding of accounting & IC system
- Evaluation of inherent & control risk & assessing audit risk
- Design & performance of test of controls & substantive procedures appropriate to meet audit objective

- Process to Initiate, process, record, report & correct transactions

- Determine flow of transactions & audit trail

SAS 94(AICPA) - Effect of IT in consideration of IC in a FSA

Risks posed by IT to IC –

1)Reliance on systems or programs that inaccurately process data, process inaccurate data, or both.

2) Unauthorized access to data resulting in destruction of data, improper changes to data, recording of unauthorized, nonexistent transactions, inaccurate recording of transactions.

3) Unauthorized changes to data in master files.

4) Unauthorized changes to systems or programs.

5) Failure to make necessary changes to systems or programs.

6) Inappropriate manual intervention.

7) Potential loss of data.

Era of the faceless customer

1. Interest Income & Expense is calculated through the system
2. Multiplicity of delivery systems like ATM / EFT / Internet & Mobile Banking / Debit & Credit cards
3. Integrity of data moving through data interfaces between various systems & software
4. Risk of override of controls through privileged access
5. Segregation of duty issues due to access to multiple systems granted to users
6. Extensive use of 3rd party outsourced vendors in data processing & management of IT infrastructure

Knowing the right reports

- Overall IT policy, Structure & environment
- Data processing & data interface under various systems
- Data integrity & security
- Business Continuity & Disaster recovery
- Controls over creation / modification of account heads & codes
- MIS reports generated & periodicity thereof
- Hard copies generated & periodicity thereof
- Exception Reports generated
- IT issues noted – resolved / unresolved last year
- Customer complaints wt errors in their transactions
- Significant observations in system audit reports

Controls

- Preventive Controls – prevent the issue from occurring or minimize the probability of the unlawful event from taking place – e.g. Security Controls
- Deterrent Controls – punitive measures in policies to deter people from committing unlawful activities
- Detective Controls – immediate arrest of damage post detection to minimize the impact
- Corrective Controls – help recovery of services / information post the event / disaster – e.g. BCP
- Entity level Controls Design & operating effectiveness
- Monitoring of Controls
- Sensitization & awareness / knowledge of controls

Getting the right reports

- Availability of authorized, accurate & complete data for processing
- No loss of data in case of interruption of power supply or processing failure
- System prevents unauthorized amendments to programs
- Appropriate access & authorization rights
- Activity log review to test segregation of duties
- Authentication of parameter changes at master or user level
- Controls on modification of Account Master
- Exception reports – generation / verification
- Inventory of IT assets – Hardware / Software obsolescence
- Input – Output & Processing Controls
- Interface – Data integrity & File continuity controls

Issues – handled usually at HO

- Email etiquette policy
- Email security
- LAN / WAN / MAN security
- Operating system security
- Archived data security
- Incidence Management policy – Information Security Officer
- Handling of confidential information & security incidents
- Privacy issues for outside agencies
- Web site security
- Persons responsible for implementing security policy & consequence for wilful violation of security Policy
- IS audit guidelines
- Vendor Selection & management
- User manuals & source codes - super users – ID disablement

Audit techniques do not change

- All modules of software are implemented
- GL codes are duly authorized & used
- Tally of GL / subsidiary books
- Controls over Passwords
- Version Controls
- Back up process – Periodicity / Storage / Custody / Retrieval & testing – Security & location
- Use of latest version of anti virus controls
- Use of security patches as & when released
- Access rights to only authorized personnel

Risks

- Transactional or Operational Risk - Processing errors -Frauds - System disruptions - unanticipated events affecting ability to deliver products & services – Policies, controls in place to mitigate risks - Documentation of risks & controls
- Credit Risk (online credit applications, submission of information & approval of loans - online tracking/ monitoring)
- Compliance – Legal Risk (E-agreements - online communications – confirmations, Document scanning)
- Reputational Risk - Identification of cyber risks - Developing cyber intelligence - increase in online communications & transactions, use of social media.

Mobile banking

- RBI Master Circular – Mobile Banking transactions in India – July1st, 2015 –
- Authentication of MPin
- Security framework - Encryption – Maintaining at all times, Confidentiality/ Integrity & availability of data – Controls to ensure there is no tampering of data & interception & change of data – security level controls at service providers
- Regulatory compliance – KYC / AML – Transactions up to Rs 5000/- can be facilitated without end to end encryption as per 4th May, 2011 RBI circular
- Need for standardization of on boarding of customers for mobile banking – 4th December 2014, RBI circular

Issues

- TDS Calculations
- NPA identifications & provisioning
- Depreciation Workings
- Alert generation for suspicious transactions – White Listing
- Due date alerts – Minor to Major – Senior citizen date - Expiry of passport & insurance policy - Limit expiry report - Document validity & file movements - receipt of stock statements, audited financials – Computation & updation of draw power - Floating interest rates – Non renewed accounts - TOD reports – Flagging dormant accounts & activation - Account Risk Profiling - Negative balance reports – Cheque Bouncing -

Are these reports readily available

- % of cash withdrawals / deposits to total
- Account Turnover as a % to Projected Sales – > 40% deviation
- > 20% Deviation of stocks - Debtors - Creditors to audited financials & as verified by stock auditors
- Number of days account was overdrawn
- Number of times TOD granted & time taken to regularize TOD
- % of limit utilization to sanctioned limit
- Secondary Collateral Value as a % of sanctioned Limit
- Date of last valuation / Inspection - Accounts not inspected
- Monitoring of audit issues – Open / Closed
- Number of days cash balances > Retention limits
- Insurance cover as a % to Average stocks held
- Dates of changes in Interest rates for Deposits / Advances

Issues

- Clearance of suspense accounts – outstanding > 7 days
- Debits in Income & credits in expense accounts
- Overdue reports – Term loan repayment debits to CC accounts – Policy in last 3 months –
- Fund Transfers in/ out related & other accounts
- Credits to NRE / FCNR accounts
- Monthly listing of Deposit/ Advances – Position on 20th March - 7th April
- Issuance & cancellation of inventories - Loose cheque leaves
- Capture & control of specimen signatures
- Asset Liability Classification Bucket wise
- Capital adequacy classification
- Error free data migration from one platform to another – No pending unresolved issues –
- Root cause / pattern analysis for errors noted – Number analytics

Issues

- Interest rate modifications – interest application skipped
- Lien marking of FDR
- Error reports
- Down time registers
- Log registers for change in product parameters
- Restrictions on usage of Pen drives / CD access
- Access to server rooms – Logs
- Annual Maintenance Contracts – Due date monitoring
- Software Licenses wrt Machines at Branch
- Insurance
- Fire Extinguishers – Due date of refilling
- Day begin & Day end activities – especially day end on 31st March

Audit techniques – don't change

- **Inquiry**
- Confirmation
- Observation
- Calculation & Re-calculation
- Reconciliation
- Physical verification & Re-verification
- Computation
- Performance & Re-performance
- Analytical procedures

Reports should be made available

- Credits lower than interest debits – need to go through the entire account statements
- Rounding offs in overdue reports – 2.9 or 3.1 to 3
- Min Max statements – effects of cheque bouncing captured on Day 2 / transfers next day – reversals
- PDC issued reducing Creditors
- Stock booked on receipt while Creditors booked on receipt of invoices
- Debtors booked on average Sales realization
- Differences in audited statements / stock statements due to year end adjustments made by auditors
- Differences in stock audit figures & borrower submissions due to timing differences – delays in data up-dation –data with CA
- **Logic used in report compilation is important**

Committee Reports

- Jilani Committee 1995 – identified various risks associated with IT systems & recommended control measures to address those risks
- Burman Committee report on IT security - 24th Dec 2002 classified 5 categories of risks in IS environment & gave a detailed checklist
- Gopal Krishna Working Committee report dtd 21st Jan 2011on 9 areas -IT Governance, Information Security, IS Audit, IT Operations, IT Services Outsourcing, Cyber Fraud, Business Continuity Planning, Customer Awareness programmes and Legal issues
- High Level Committee for preparation of Information Technology Vision Document : 2011-17 – 28th Feb, 2011
- Talwar Committee Report - 3rd August 2011 -Chapter on Technology & Customer Service
- TRAI – Mobile Banking (Quality of Service) Regulations, 2012

15 areas – Burman Committee

Business Strategy
Long Term IT Strategy
Short Range IT Plans
IS Security Policy
Implementation of Security Policy

IS Audit Guidelines
Acquisition and Implementation of Packaged Software
Development of software - in-house and outsourced
Physical Access Controls
Operating System Controls
Application Systems Controls
Database controls
Network Management
Maintenance
Internet Banking

International frameworks

- **COBIT 5** - Control objectives for information and related technology – April 2012 framework of best practices created for IT management & governance by ISACA (Information Systems Audit & Control Association)
- **ISO/IEC 27002** – Information Security Standard of ISO (International Organization for Standardization) - Best practices to initiate, implement, or maintain Information Security management systems (ISMS).
- Information security –
- *Preservation of Confidentiality ensuring that information is accessible only to those authorized to have access)*
- *Integrity (safeguarding the accuracy and completeness of information and processing methods)*
- *Availability (ensuring that authorized users have access to information & associated assets when required)*

NIST SP 800 30 framework – Sept 2012

9 step Guidance for conducting risk assessments

- Step 1 System Characterization
- Step 2 Threat Identification
- Step 3 Vulnerability Identification
- Step 4 Control Analysis
- Step 5 Likelihood Determination
- Step 6 Impact Analysis
- Step 7 Risk Determination
- Step 8 Control Recommendations
- Step 9 Results Documentation

Risk Mitigation

- **Risk Assumption -** Accept the potential risk & continue operating the IT system or implement controls to lower the risk to an acceptable level
- **Risk Avoidance** - Avoid the risk by eliminating the risk cause &/or consequence (e.g., forgo certain functions of the system or shut down the system when risks are identified)
- **Risk Limitation -** Limit the risk by implementing controls that minimize adverse impact of a threat's exercising a vulnerability (e.g., use of supporting, preventive, detective controls)
- **Risk Planning -** Manage risk by developing a risk mitigation plan that prioritizes, implements, & maintains controls
- **Research & Acknowledgement -** Lower risk of loss by acknowledging the vulnerability or flaw & researching controls to correct the vulnerability
- **Risk Transference -** Transfer the risk by using other options to compensate for the loss, say purchase of insurance.

Issues

- Multiple customer ID's – same PAN / Email Id / Address / Phone
- Data cleansing – Data purification – SBI Project Ganga
- Information Technology Act, 2000
- Garbage In – Garbage Out
- IT general Controls
- VAPT – Vulnerability assessment & penetration testing
- Software application is as accurate as it is programmed to be
- Data thefts
- Frauds
- FATCA – CRS
- Training / Awareness

Frauds

- **Hacking or Cracking** - illegal intrusion of information in a computer system & or network.

- **Phishing** - acquiring of sensitive information such as user names, passwords or credit card details by masquerading as a trustworthy entity in an electronic communication.

- **Vishing and Smishing** - Phone scams similar to "phishing". Vishing is a telephone call claiming to be from a legitimate company requesting personal information to resolve an urgent financial matter unfortunately the telephone call is phony & you are providing information to a fraudster. Smishing is done through text messages on a cell phone by asking you to call a particular number or click on a link that could contain malicious code & potentially steal information stored in your cell phone without your knowledge.

- **Data theft** - use of hand held devices like flash drives, I pods, digital cameras & ability to transmit large amounts of data quickly vide e-mail, web pages, USB drives, DVD storages & other hand held devices.

Frauds

- **Impersonation:** Imposter obtains key pieces of personal information to impersonate someone else. He assumes identity of that person to make transactions, purchases, get loans or credits. Done for illegal immigration, hiding from creditors or people who want to be anonymous for personal reasons. person whose identity is assumed suffers various consequences as he is held responsible for the perpetrators actions.

- **Botnets - N**etworks of compromised computers, controlled by remote attackers to perform illicit tasks as sending spam or attacking other computers.

- **Malvertising – M**ethod whereby users download malicious code by simply clicking at some advertisement on any infected website

- **Cyber Extortion**: Blackmailing the victim & extorting money to stop the DOS attacks or give back the information stolen or discontinue vandalism. **Cyber Terrorism - Warfare**: Distributed Denial of service attacks, hate websites & hate emails, attacks on service network etc. **Computer Vandalism** is damaging or destroying data instead of stealing or misusing it. Programs used attach themselves to a file & circulate.

- **PUPs (Potentially Unwanted Programs) -** installs unwanted software in system like search agents, toolbars.

Frauds

- **E mail spoofing - S**ending an email to another person in a way that it appears that the email was sent by someone else. Mail appears to originate from one source but is actually sent from another source.
- **Denial of Service or DOS** attacks flood the bandwidth of the victim's network or fills his e mail box with spam mail depriving him of service that he is entitled to access or provide.
- **Dissemination of viruses** by use of malicious software that attaches itself to other software. Some common viruses are Virus worms, Trojan horse, Web jacking, Email bombing.
- **Software piracy** Theft or illegal copying of genuine programs or by counterfeiting & distribution of product intended to be passed as originals.
- **Misuse of Digital Signature:** If the private key is not stored securely, it can be misused without knowledge of Private key owner to issue unauthorized digital certificates for cyber espionage, malware diffusion or sabotage.
- **Man in the Middle Attacks (MITM)** - Attacker secretly relays & possibly alters communication between 2 parties who believe they are directly communicating with each other. Attacker intercepts all messages between the 2 victims and injects new ones & in fact controls the entire conversation.

Card Frauds

- Use of Debit or Credit cards to obtain goods without paying or obtaining unauthorized funds from an account.
- Using fake identities, documentations, impersonation to get genuine cards
- Using a stolen or lost Credit card for illegal purchases before the holder notifies the issuing bank & the issuing bank puts a block on the account
- Skimming or theft of payment card information used in a legitimate manner by using basic methods like photocopying receipts or advanced methods like using small electronic devices (skimmers) to swipe & store hundreds of victim card numbers.
- Tele Phishing is obtaining a list of individuals with their name & phone numbers luring victims into thinking that they are speaking with a trusted organization while handing over sensitive information such as card details.

Card Frauds

- A Merchant at a POS (Point of Sale) terminal allowing a fraudster to get goods on a stolen credit card for consideration. Providing details of customer cards to a fraudster for consideration. Conniving with a fraudster & allowing him to substitute the imprinter to collect data, then used to multiply cards.

- Swiping of a card by a merchant for a nonexistent transaction & accommodating another by lending money from transaction value received from the paying bank.

- Card holder declaring card as stolen or lost to the issuer & soon after use it himself to it's limits. Loss on the card post intimation is the banker / issuer loss.

- Various credit cards are applied simultaneously at the same time by a fraudster with no previous default history & with intent only to use the card to the fullest & not repay or at times agree to an OTS of the dues at a much lesser amount than owed

Conclusion

- Are we aware of what is CBS risk
- Is the Branch head & staff aware of IT risks
- Is there an IT policy in place circulated, read & understood by all –
- Are system audit reports available
- Is Network configuration diagram available
- Is there a Fraud policy
- ICOFR – is it known
- Please report factually – state extent & manner of checking done –
- Assumption is the mother of all goof ups

Back up slides

- Data Centre - A centralized repository for storage, management & dissemination of data & information.
- Down Time - Time during which a machine, especially a computer, is out of action or unavailable for use.
- Computer or data network is a telecommunications network which allows computers to exchange data.
- Network connectivity describes the extensive process of connecting various parts of a network to one another, for example, through the use of routers, switches and gateways, and how that process works.
- **Server** is a computer program or a device that provides functionality for other programs or devices, called "clients
- **Web application** (**Web app**) is an application program that is stored on a remote server and delivered over the Internet through a browser interface

Back up slides

- **Interface** is a shared boundary across which 2 separate components of a computer system exchange information. i.e. say between software, hardware, peripheral devices, humans & combinations of these. Touch Screen, a Hardware device can send & receive data through the interface, while a mouse, microphone or joystick are one way only
- **Immediate Payment Service** (IMPS) of India started in Nov 2010 offers an instant, 24X7, interbank electronic fund transfer service through mobile phones. MPIN is a 4-digit code used to authenticate IMPS transactions
- VAPT tools provide a detailed picture of the flaws that exist in an application & the risks associated with those flaws

Back up slides

- **ITGC or General Computer Controls (GCC)** - Controls, other than application controls relate to the environment within which computer-based application systems are developed, maintained & operated & are applicable to all applications. They ensure proper development & implementation of applications, integrity of program, data files &of computer operations.
- Logical access controls over infrastructure, applications, & data.
- System development life cycle controls.
- Program change management controls.
- Data center physical security controls.
- System and data backup and recovery controls.
- Computer operation controls.

GTAG – IIA

- GTAGs are written to address issues related to information technology (IT) management, control, & security.
- **GTAG 1:** Information Technology Controls
- **GTAG 2:** Change and Patch Management Controls: Critical for Organizational Success
- **GTAG 3:** Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment
- **GTAG 4:** Management of IT Auditing
- **GTAG 5:** Managing and Auditing Privacy Risks
- **GTAG 6:** Managing and Auditing IT Vulnerabilities
- **GTAG 7:** Information Technology Outsourcing
- **GTAG 8:** Auditing Application Controls

GTAG – IIA

- **GTAG 9:** Identity and Access Management
- **GTAG 10:** Business Continuity Management
- **GTAG 11:** Developing the IT Audit Plan
- **GTAG 12:** Auditing IT Projects
- **GTAG 13:** Fraud Prevention and Detection in the Automated World
- **GTAG 14:** Auditing User-developed Applications
- **GTAG 15:** Information Security Governance
- **GTAG 16:** Data Analysis Technologies
- **GTAG 17:** Auditing IT Governance

Application controls

- Controls over input, processing, &output functions
- Ensures –
- Input data is complete, accurate & valid
- Internal processing produces expected results
- Processing accomplishes desired tasks
- Output reports are protected from disclosure
- Include –
- Edit tests
- Control totals/ Batch balancing
- Reconciliation of accounts
- Exception handling

Application Controls

- Input Controls –

  Input Authorization

  Batch Controls & Balancing

  Error Reporting & Handling

  Batch Integrity in Online or Database systems

- Processing Controls – Data Validation and Editing Procedures Sequence check - Limit check - Range check - Validity check - Reasonableness check - Table lookups - Existence check - Key verification - Check digit - Completeness check - Duplicate check - Logical Relationship check

  Processing Controls

  Data File Control Procedures – Parity checking - Transaction logs - Version usage - File up-dation & maintenance authorization

Application controls

- Output Controls –

  Was the information distributed to the appropriate recipient?

  Where was the sensitive report printed?

  Was distribution controlled?

  How long are sensitive reports retained & stored in a protected environment?

  Are they protected from disclosure &confidentiality.

  Batch - Quantity required for or produced as the result of one operation

  RTO - Amount of time the business can be without the service, without incurring significant risks or significant losses (Point Objective)

  RPO - maximum targeted period in which data might be lost from an IT service due to a major incident (Time Objective)

On line Audit Techniques

- Systems Control Audit Review File & Embedded Audit Modules (SCARF/EAM) – log created to collect information for subsequent review & analysis
- Snapshots give an audit trail like taking a lot of snapshots & placing them end to end to analyze the processing logic of specific programs
- Audit hooks for those low complexity tasks which mark questionable or suspicious transactions on real time basis as Red Flags
- Integrated Test Facility creates a fictitious entity in a database to process test transactions simultaneously with live input
- Continuous and Intermittent Simulation verifies processing of actual transactions to verify with actual client results

Audit Software

Popular software - Audit Control Language (ACL) & IDEA (Interactive Data Extraction and Analysis)

ACL - Data interrogation tool used by auditors to view, explore & analyze data efficiently & cost effectively. ACL enables auditors to access data in diverse formats and on various types of storage devices.

IDEA - Generalized Audit Software which imports a wide range of different types of data files. During the import an IDEA file & its field statistics are created.

New developments

- BSCBI (Banking Codes & Standards Bureau of India)
- Customer Grievance Cells & Banking Ombudsman
- Cheque Truncation system
- Banca Assurance
- Umbrella Banking
- Tablet Banking
- RBI - OSMOS returns (offsite monitoring & surveillance)
- IDRBT - Institute for Development & Research in Banking Technology
- INFINET – Indian Financial Network

New developments – Go Green

- Energy efficient data centers
- Low energy consuming computing devices
- SaaS - Software as a service solution
- New technologies - Cloud computing - VPN - Server & storage virtualization
- LCD monitors rather than CRT monitors
- Reduction in paper usage –using emails / attachments
- Waste management – reduce, reuse & recycle
- Tele commuting – Web conferencing
- Duplex Printing / Multi page printing / sleep mode

Success Trains – Failure Complains

- People are losing curiosity & the desire to learn & improve themselves & that in complacency & self satisfaction lies a low descent into mediocrity.
- The more you learn you learn that you still have a lot to learn – Learn – Unlearn – Relearn -
- We can not solve our problems with the same level of thinking that created them – Albert Einstein
- If you want something you have never had, then you got to do something that you never did