



Operations Management

CGBS/CARTAC IT Workshop for Regional Bank Examiners

June 23 – 25, 2009
Georgetown, Guyana

David A. Wong
Senior Systems and Technology Officer
Financial Institutions Supervisory Division
Methods, Analysis and Quality Review Department
Bank of Jamaica
www.boj.org.jm



Agenda

- Operations: Main Tasks
- Inside IT Operations (Hardware/Software)
- Database Management Systems
(DBMS ->DBA)
- Networks and Communication

Agenda

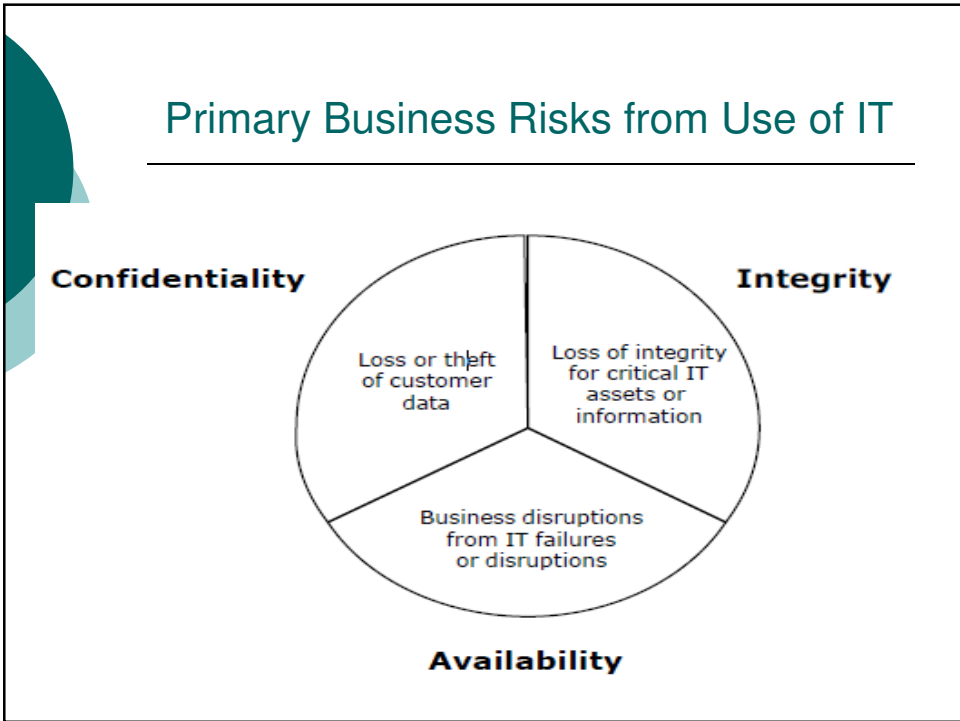
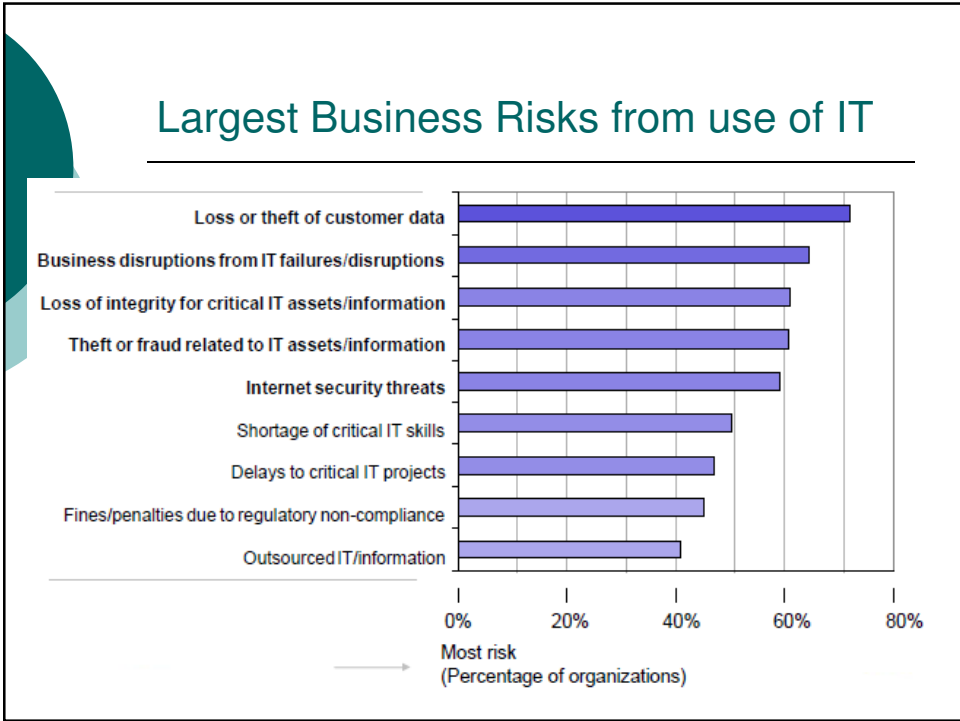
continued

- IT Operations: Documentation
- Problem management
- Key Examiner Notes

Operations: Main Tasks

Main operational activity includes:

- Running Jobs (automated / manual processes)
- Backup / distribution of media, software and reports
- Managing computer facilities and security efforts
- Adhering to job schedules (EOD processes and run batch jobs)
- Help desk / Support



Inside IT Operations: Hardware

Types of Computers:

- Mainframes - typically serves 100-400 users and usually occupies a special air conditioned room
- Mini and Microcomputers - designed around a microprocessor and used by one person at a time
- Notebooks - small portable personal computer
- PDA / Smart phones - (personal digital assistant), handheld computer device or mobile phone with advanced capabilities

Hardware Maintenance

For effective risk mitigation IS departments should:

- have a schedule
- Document work done and results
- ensure activities fall within budget
- ensure maintenance is performed by a reputable vendor

Hardware Monitoring

For effective monitoring three main reports include:

- Error Reports - this lists any failures
- Availability Reports - this tracks downtime
- Utilization Reports - this tracks CPU and Disk usage, sessions and peripherals

Capacity Planning

- Involves baseline performance data to model and project future needs
- Closely integrated with the budgeting and strategic planning process
- Includes training, number of users and internal factors (eg. growth, acquisitions and mergers)



Inside IT Operations: Software Architecture

System Software includes:

- Operating Systems
- Access Control Software
- Data Communications Software
- Database Management Software
- Network Management Software
- Etc.



Data Communication Software

Examiners are to be interested in:

- The Transmitter (source)
- The Transmission Path (line or channel)
- Receiver (the sink)



Database Management Systems (DBMS)

- Used to configure and operate databases
- Databases pose unique risks as FI's repository of it's most critical information
- Failure to adequately manage and secure can lead to unintentional or unauthorized modification, destruction or disclosure of sensitive information
- Risks may spiral from operational risk ->reputation risk ->legal risk



Database Management Systems (DBMS)

continued

DBMS's essentially:

- Allows the application to access the data
- Controls access to data
- Manages the Data

The Database Administrator (DBA)

- Monitors the database
- Complements IS function
 - Databases and DBMSs are often targets of malicious activity by both internal and external sources)
- Manages the database (unique views and test environments)

Database Administration Risks and Risk Mitigation

RISKS:

- An administrator can alter data without those modifications being detected
- An administrator can change access rights to information stored within the database, as well as their own access rights

RISK MITIGATION (*preventative and detective*):

- Restrict and review access administration and data altering by the administrator
- Close monitoring of DBA activities by management

IT Operations: What is a Network?

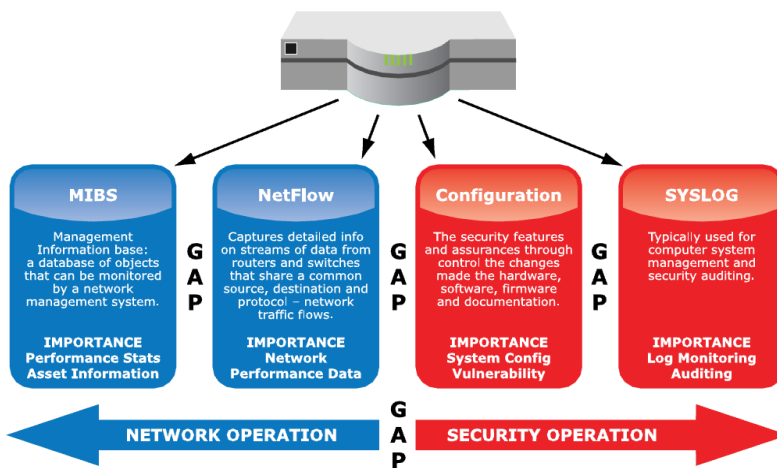
"A collection of devices and procedures for communicating and sharing information over distances"

LAN, WAN, PROXY SERVER, ROUTER,
 SWITCH, FIREWALL, BANDWIDTH,
 PACKETS, INTERNET, INTERNAL NETWORK,
 DATA CENTER, PORT, PROTOCOL, IP ADDRESS,
 DE-MILITARIZED ZONE (DMZ), HONEYPOT, IDS,
 IDPS, SERVER



goodwarriors.mpeg

The Challenge to Every Organization



Common Consequences of these Gaps

Apart from the inherent risks in each module, gaps may lead to:

- Legal and Regulatory Risk
 - can entail financial liabilities in the form of fines and restriction
- Operational Risk
 - due either to deliberate malfeasance or human error.
 - can lead to enormous costs resulting from lack of system availability or loss of revenue.
- Reputational Risk
 - associated with a loss of customer or public confidence

Network Management Tools

“Different FI’s use different network management tools”

The common measurements are:

- Latency
 - time taken for a packet to travel from source to destination
- Throughput
 - amount of data transferred from one place to another

Network Monitoring

Networks are monitored using:

- Response Time Reports
- Downtime Reports
- Help Desk Reports

*based on the specific tools used and the purpose of the network

IT Operations: Documentation

- Operator Instructions
 - includes the procedural manuals that guide the various processes and activities
- Error Handling Instructions
 - Eg. explains what to do when different errors or exceptions are encountered
- Library Management
 - includes the detail technical documentation and how they are maintained
- Output Distribution
 - relates to how the output (reports) are disseminated throughout the organization



Service Level Agreements (SLA)

- Exists between IT and users
- They establish performance objectives
- They are aligned with users' business requirements
- Important when services are outsourced



Event/Problem Management

The plan should cover:

- Hardware
- OS
- Applications
- Security Devices

Ensuring that:

- All problems are logged
- Escalation procedure exist
- Resolutions are tracked
- Each entry has complete documentation

"Essentially, an effective process, helps to protect institutions from financial loss, operational and reputation risks"

Examiner Key Point

Be keen to:

- Review inventory listings
- Review system diagrams and topologies
- Ensure daily operational controls and processes exist (eg. Scheduling activities, monitoring, etc.)
- Ensure appropriate segregation and rotation of duties
- Review organization structure is appropriate
- Ensure environmental controls are in place (eg. Sufficient electrical power, cooling, telecommunication, etc.)
- Ensure appropriate logical and physical security controls exist

IT Operations: Today's Challenge



Questions



David A. Wong
Senior Systems and Technology Officer
FISD/MAQR
Bank of Jamaica

CGBS/CARTAC Regional IT WORKSHOP

Resources

- FFIEC IT Management Handbook
- FFIEC IT Operations Handbook
- ISACA Review Notes
- Federal Reserve Bank of Chicago –STREAM Tech Lab

Resources

White Papers:

- Complying with Financial Services Regulations Through Information Availability by Vision Solutions
- IT in the Financial Sector – the Key to Thriving in a Challenging Economy by Don Jones
- Pillars of Application Quality: Security, Functional, and Performance Testing sponsored by HP