East AFRITAC
INTERNATIONAL MONETARY FUND
REGIONAL TECHNICAL
ASSISTANCE CENTER

East AFRITAC, East Afrtac
P.O. Box 10054
Dar es Salaam, Tanzania

Tel: 255-22-223-5353
Fax: 255-22-223-4204

Web site: www. eastafritac.org
Building macroeconomic capacity in East Africa

INTERNATIONAL ★ MONETARY FUND ★

International Monetary Fund
East AFRITAC

Program

Seminar on Information Technology Risk Supervision
September 15 – 16, 2016

Thursday September 15	
08:30 - 08:45	**Registration**
08:45 - 09:00	**Session 1 – Opening** *Deputy Governor Bank of Tanzania (To be confirmed)*
09:00 – 09:30	**Session 2 – Context workshop** *Facilitator: Dirk Jan Grolleman (IMF East AFRITAC)*
09:30 – 10:45	**Session 3 – International Approach to Technology Risk Supervision** *Facilitator: Abhilash Bhachech (IMF Expert)*
10:45 – 11:00	**Q&A**
11:00 – 11:30	***Break***
11:30 – 12.45	**Session 3 – Regional Approach to Technology Risk Supervision** *Facilitator: Dercio Mutimucuio (IMF expert)*
12:45 - 13:00	***Q&A***
13:00 - 14:00	***Lunch***
14:00 - 15:00	**Session 4 – External IT Audit (KPMG)** - Scope and depth of the IT Audit - Work and views on outsourcing (within the group mostly) and centralized core banking systems and functions - Views on the main risks and the development of IT/Technology risk in the region - Experiences in engaging with supervisory authorities (bilaterally or trilaterally)
15:00 – 15:15	**Q&A**
***15:15* - 15:45**	***Break***
15:45 - 16:45	**Session 5 – Forensic Audit (KPMG)** - When is forensic audit experience needed (in the banking sector) and to what extent does it differ from regular audit and supervisory expertise - What are indicators supervisors could use for assessing whether not to

	involve forensic auditors - Views on the main risks and the development of IT/Technology risk in the region
16:45 – 17:00	**Q&A**
17:00 - 17:30	**Conclusions and wrap-up day 1**
Friday September 16	
08:30 – 08:45	**Session 1: Regional developments and challenges** *Facilitator: Dirk Jan Grolleman (IMF East AFRITAC)*
08:45 – 09.15	**Session 2: Country presentation** *(Tentative: Malawi)* - Development specialized in-house capacity - Approach towards IT/Technology Risk Supervision
09.15 – 09.30	**Q&A**
09:30 – 10:00	**Session 3: Country presentation** *(Tentative: Kenya)* - Experiences in engaging with external (and forensic) auditors in general and in relation to IT/Technology - Supervision of regionally centralized IT/core banking function of Kenyan cross-border banks - Approach towards IT/Technology Risk Supervision
10:00 – 10:15	**Q&A**
10:15 – 10:45	***Break***
10:45 – 11:15	**Session 4: Country presentation** *(Tentative: Tanzania)* - Experiences in engaging with external (and forensic) auditors in general and in relation to IT/Technology - Supervisory approach towards (regionally and internationally) outsourced core banking functions - Approach towards IT/Technology Risk Supervision
11:15 – 11.30	**Q&A**
11:30 - 12:30	**Panel discussion – Proposed way forward to deal with the challenges**
12:30 – 13:00	**Wrap-up and Closing Remarks**
13:00 - 14:00	***Lunch***

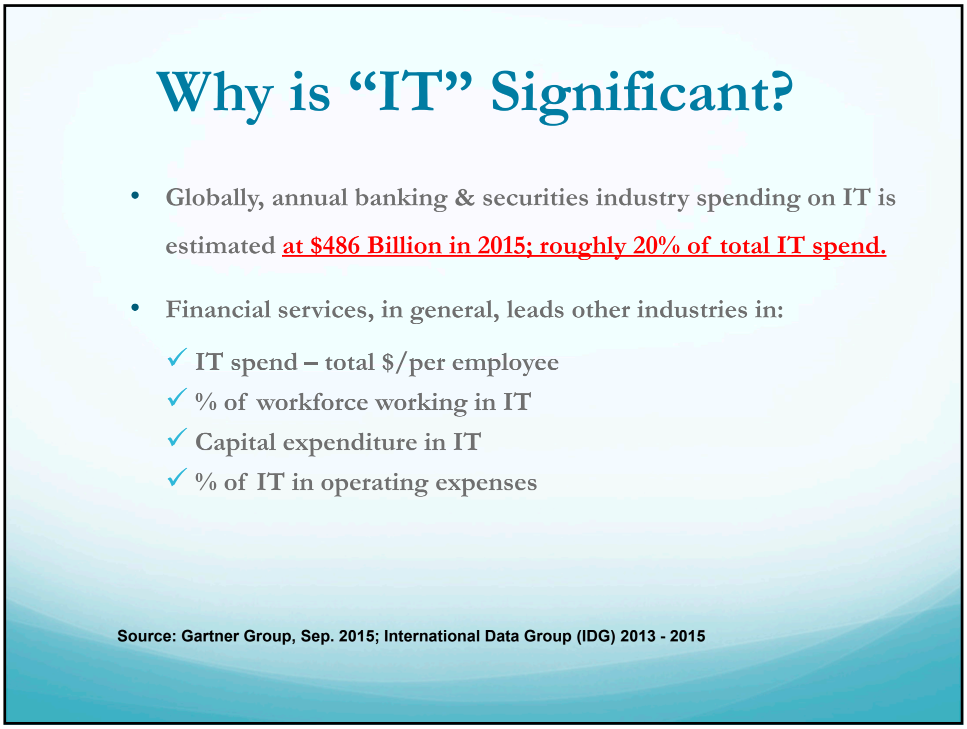
International Approach to Technology Risk Supervision

Seminar on Technology Risk Supervision
International Monetary Fund, East AFRITAC
Dar es Salaam, Tanzania
September 15th 2016

Abhilash Bhachech
Inspector of Bank & Trust Companies
Central Bank of The Bahamas

Agenda

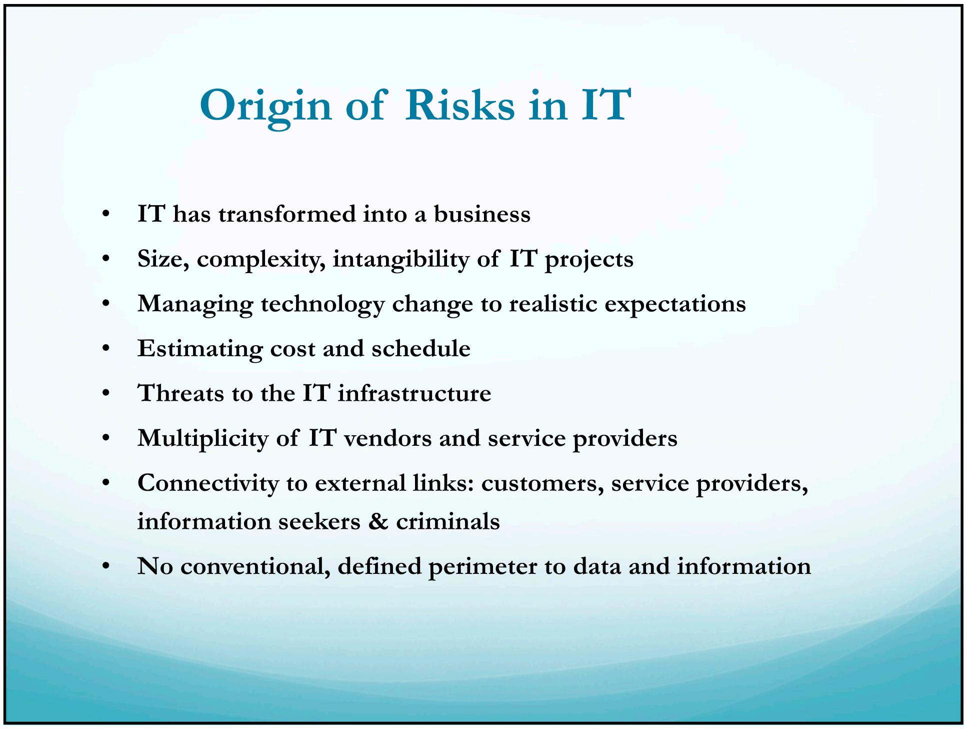
- Significance of Technology… and Risks
- Supervisory Approaches & Context
  - ✓ Basel Outcomes
  - ✓ Supervisory Approaches
  - ✓ International Co-operation
- Going Forward…
- Questions?



Why is "IT" Significant?

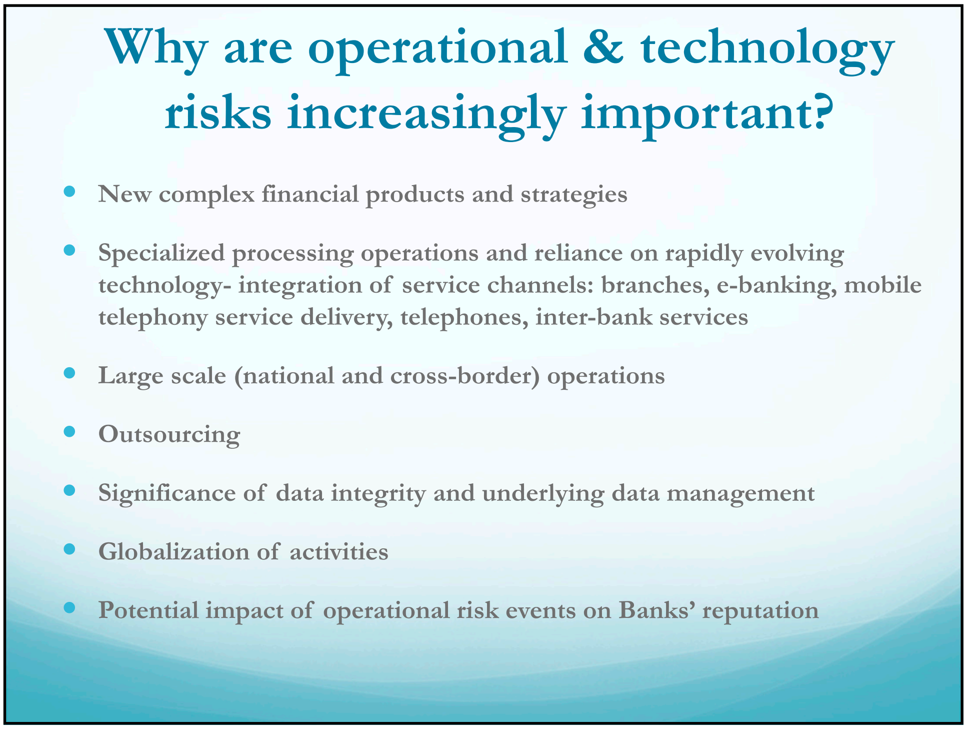
- Globally, annual banking & securities industry spending on IT is estimated at $486 Billion in 2015; roughly 20% of total IT spend.
- Financial services, in general, leads other industries in:
  - ✓ IT spend – total $/per employee
  - ✓ % of workforce working in IT
  - ✓ Capital expenditure in IT
  - ✓ % of IT in operating expenses

Source: Gartner Group, Sep. 2015; International Data Group (IDG) 2013 - 2015



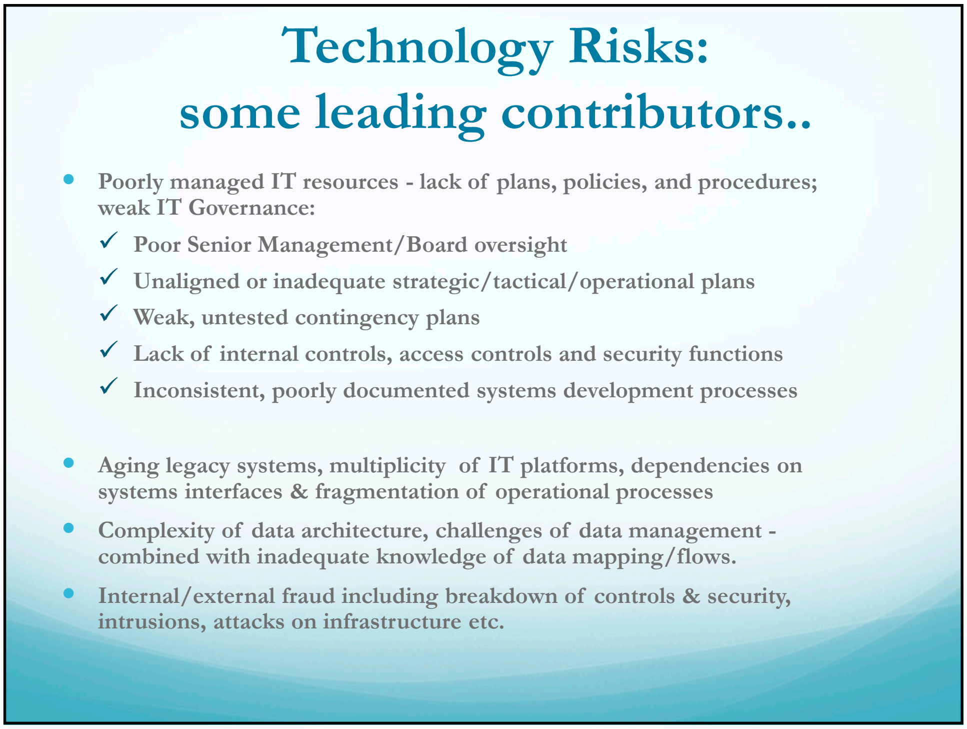
Origin of Risks in IT

- IT has transformed into a business
- Size, complexity, intangibility of IT projects
- Managing technology change to realistic expectations
- Estimating cost and schedule
- Threats to the IT infrastructure
- Multiplicity of IT vendors and service providers
- Connectivity to external links: customers, service providers, information seekers & criminals
- No conventional, defined perimeter to data and information



Why are operational & technology risks increasingly important?

- New complex financial products and strategies
- Specialized processing operations and reliance on rapidly evolving technology- integration of service channels: branches, e-banking, mobile telephony service delivery, telephones, inter-bank services
- Large scale (national and cross-border) operations
- Outsourcing
- Significance of data integrity and underlying data management
- Globalization of activities
- Potential impact of operational risk events on Banks' reputation



Technology Risks: some leading contributors..

- Poorly managed IT resources - lack of plans, policies, and procedures; weak IT Governance:
  - ✓ Poor Senior Management/Board oversight
  - ✓ Unaligned or inadequate strategic/tactical/operational plans
  - ✓ Weak, untested contingency plans
  - ✓ Lack of internal controls, access controls and security functions
  - ✓ Inconsistent, poorly documented systems development processes
- Aging legacy systems, multiplicity of IT platforms, dependencies on systems interfaces & fragmentation of operational processes
- Complexity of data architecture, challenges of data management - combined with inadequate knowledge of data mapping/flows.
- Internal/external fraud including breakdown of controls & security, intrusions, attacks on infrastructure etc.

The ‘Operational Risk’ Context

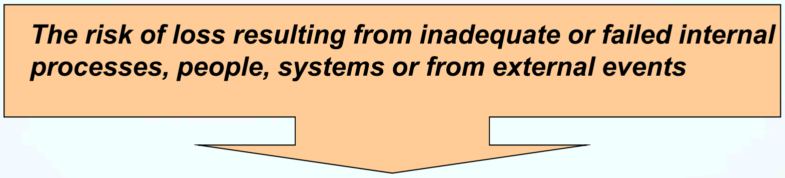
Basel Accord

- The risk of loss resulting from inadequate or failed
  - ✓ processes
  - ✓ people
  - ✓ systems

  or from external events

- Effective Basel II implementation, “Operational Risk” (including Technology Risk) is subject to attribution of a regulatory capital charge.

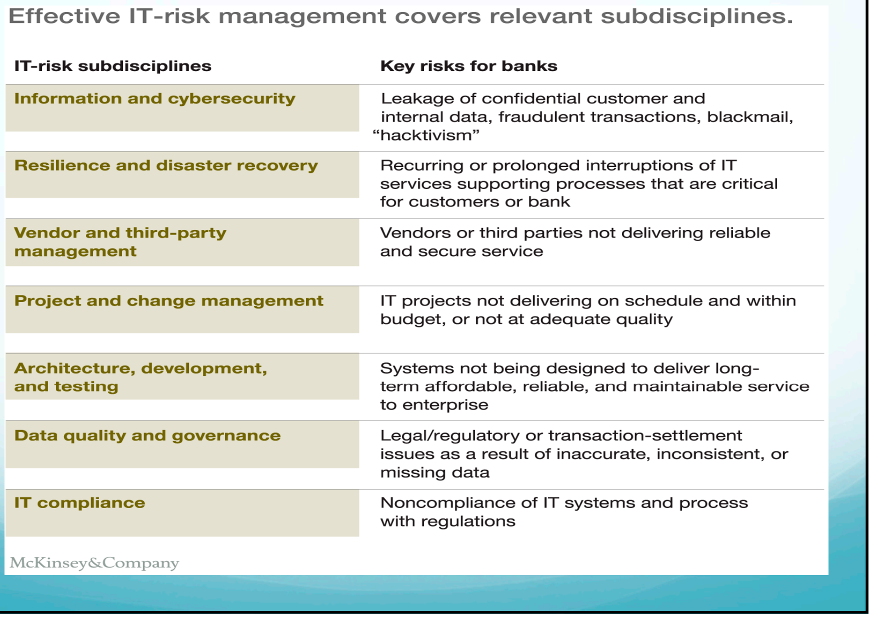
…Operational Risk – ‘Basel’ view



The risk of loss resulting from inadequate or failed internal processes, people, systems or from external events

- Internal fraud
- External fraud
- Employment practice and workplace safety
- Clients, products and business practices
- Damage to physical assets
- Business disruptions and system failures
- Execution, delivery and process management

Risk Management Coverage..



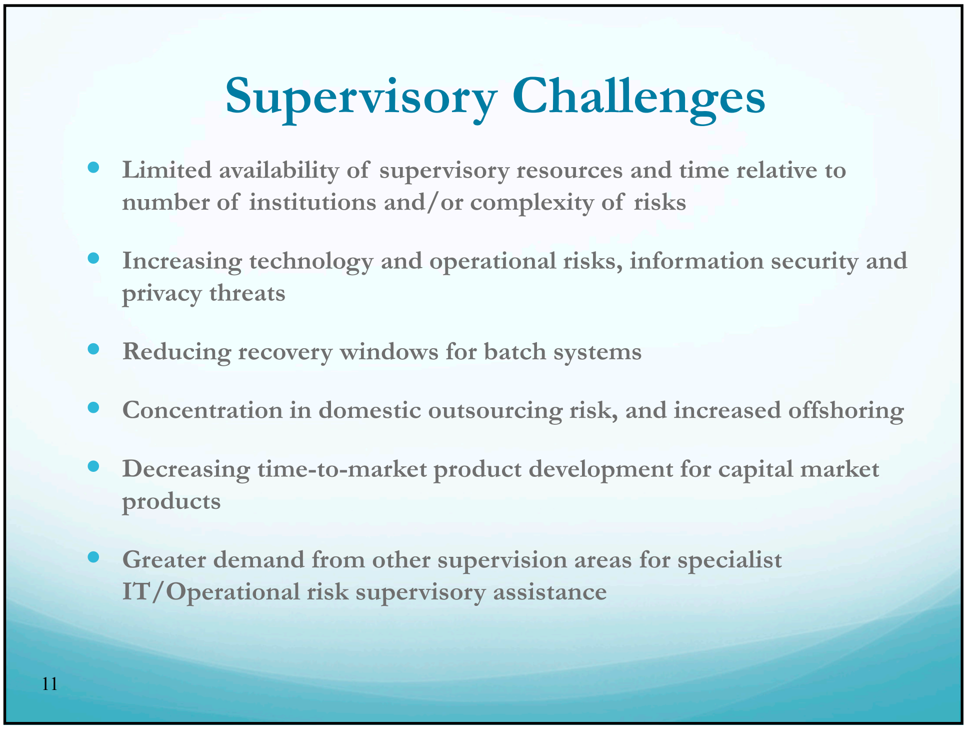
Effective IT-risk management covers relevant subdisciplines.

IT-risk subdisciplines	Key risks for banks
Information and cybersecurity	Leakage of confidential customer and internal data, fraudulent transactions, blackmail, "hacktivism"
Resilience and disaster recovery	Recurring or prolonged interruptions of IT services supporting processes that are critical for customers or bank
Vendor and third-party management	Vendors or third parties not delivering reliable and secure service
Project and change management	IT projects not delivering on schedule and within budget, or not at adequate quality
Architecture, development, and testing	Systems not being designed to deliver long-term affordable, reliable, and maintainable service to enterprise
Data quality and governance	Legal/regulatory or transaction-settlement issues as a result of inaccurate, inconsistent, or missing data
IT compliance	Noncompliance of IT systems and process with regulations

McKinsey&Company

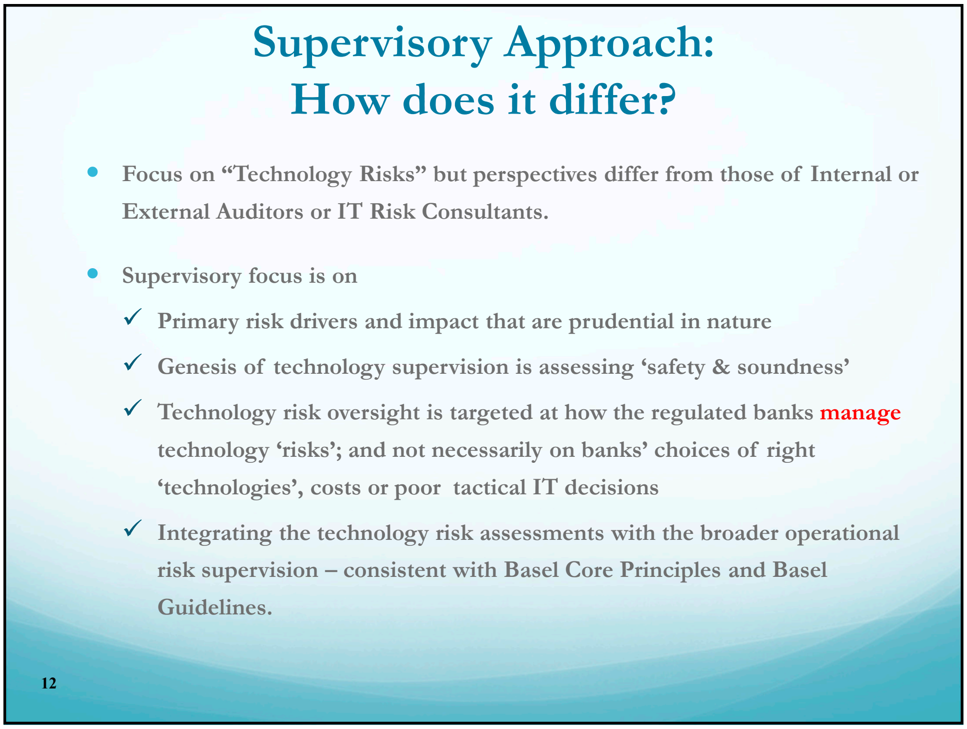
Agenda

- Significance of Technology… and Risks
- Supervisory Approaches & Context
  - ✓ Basel Outcomes
  - ✓ Supervisory Approaches
  - ✓ International Co-operation
- Going Forward…
- Questions?



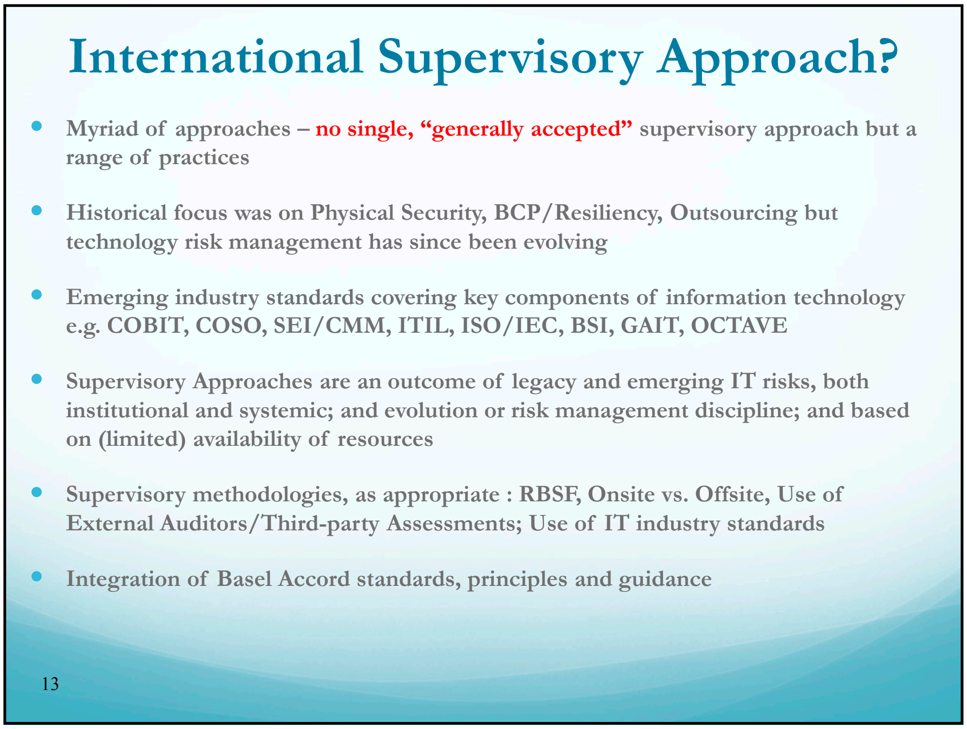
Supervisory Challenges

- Limited availability of supervisory resources and time relative to number of institutions and/or complexity of risks
- Increasing technology and operational risks, information security and privacy threats
- Reducing recovery windows for batch systems
- Concentration in domestic outsourcing risk, and increased offshoring
- Decreasing time-to-market product development for capital market products
- Greater demand from other supervision areas for specialist IT/Operational risk supervisory assistance



Supervisory Approach: How does it differ?

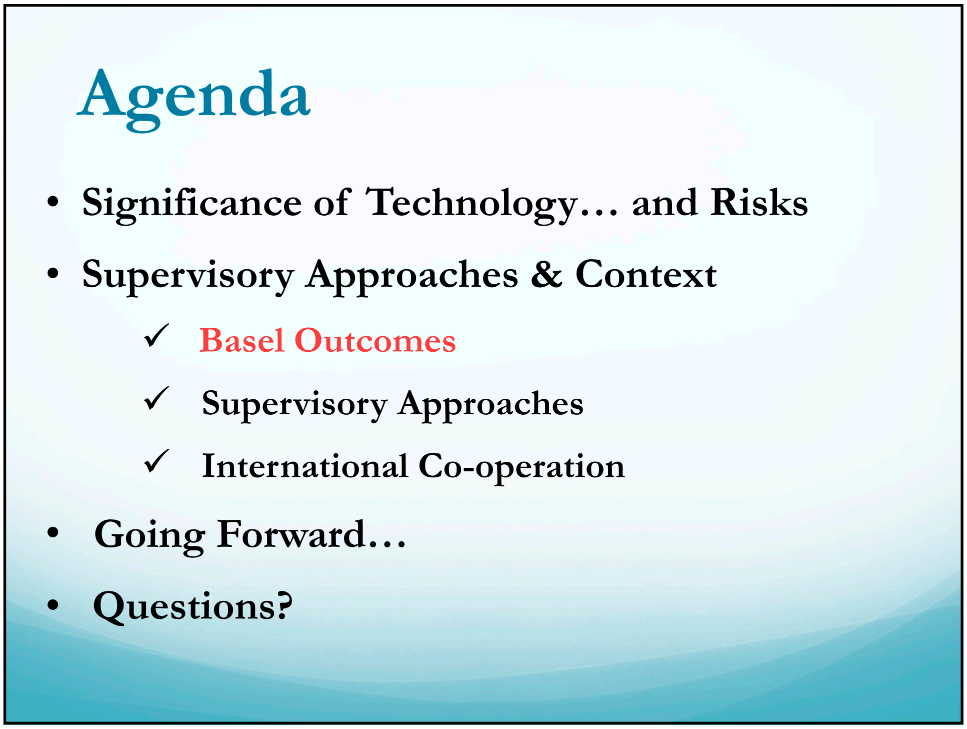
- Focus on "Technology Risks" but perspectives differ from those of Internal or External Auditors or IT Risk Consultants.
- Supervisory focus is on
  - ✓ Primary risk drivers and impact that are prudential in nature
  - ✓ Genesis of technology supervision is assessing 'safety & soundness'
  - ✓ Technology risk oversight is targeted at how the regulated banks manage technology 'risks'; and not necessarily on banks' choices of right 'technologies', costs or poor tactical IT decisions
  - ✓ Integrating the technology risk assessments with the broader operational risk supervision – consistent with Basel Core Principles and Basel Guidelines.



International Supervisory Approach?

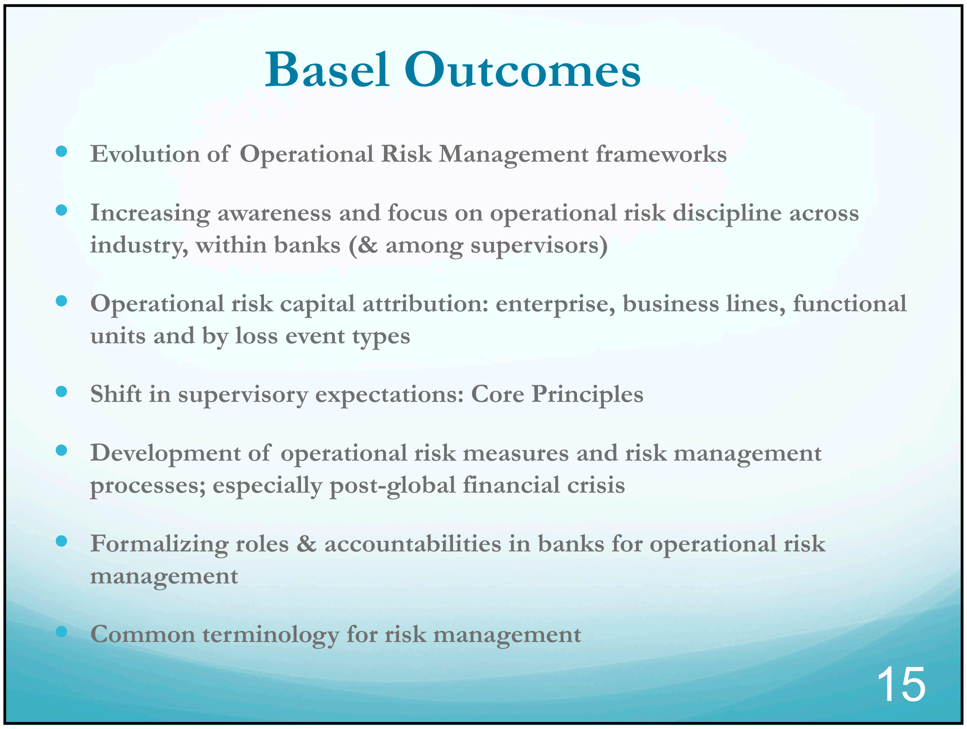
- Myriad of approaches – no single, “generally accepted” supervisory approach but a range of practices
- Historical focus was on Physical Security, BCP/Resiliency, Outsourcing but technology risk management has since been evolving
- Emerging industry standards covering key components of information technology e.g. COBIT, COSO, SEI/CMM, ITIL, ISO/IEC, BSI, GAIT, OCTAVE
- Supervisory Approaches are an outcome of legacy and emerging IT risks, both institutional and systemic; and evolution or risk management discipline; and based on (limited) availability of resources
- Supervisory methodologies, as appropriate : RBSF, Onsite vs. Offsite, Use of External Auditors/Third-party Assessments; Use of IT industry standards
- Integration of Basel Accord standards, principles and guidance

13



Agenda

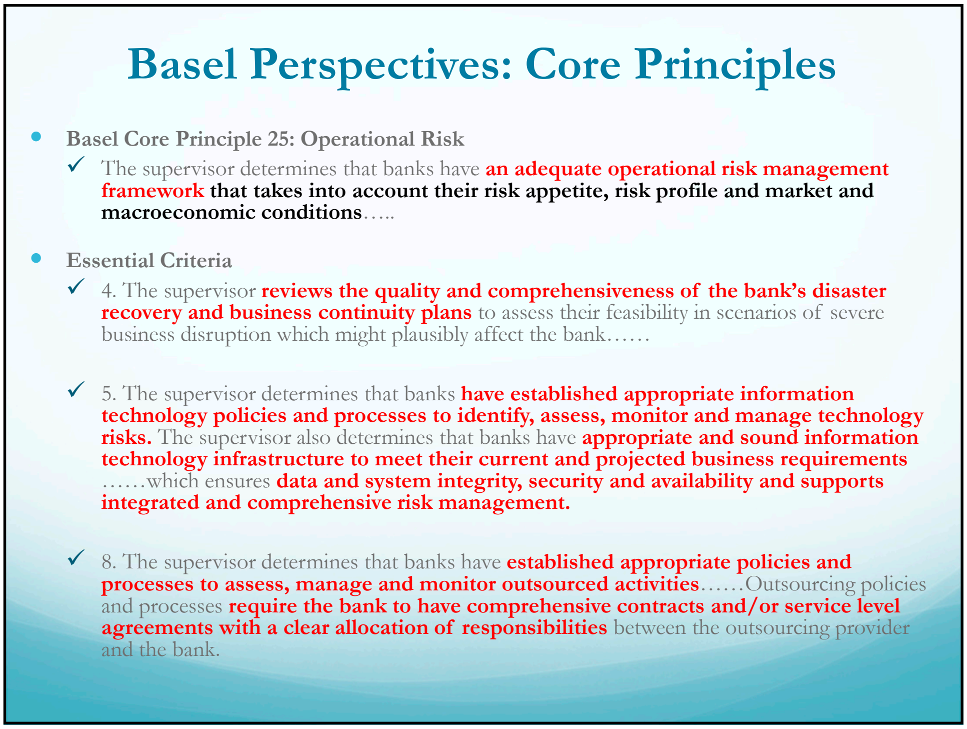
- Significance of Technology… and Risks
- Supervisory Approaches & Context
  - ✓ Basel Outcomes
  - ✓ Supervisory Approaches
  - ✓ International Co-operation
- Going Forward…
- Questions?



Basel Outcomes

- Evolution of Operational Risk Management frameworks
- Increasing awareness and focus on operational risk discipline across industry, within banks (& among supervisors)
- Operational risk capital attribution: enterprise, business lines, functional units and by loss event types
- Shift in supervisory expectations: Core Principles
- Development of operational risk measures and risk management processes; especially post-global financial crisis
- Formalizing roles & accountabilities in banks for operational risk management
- Common terminology for risk management

15

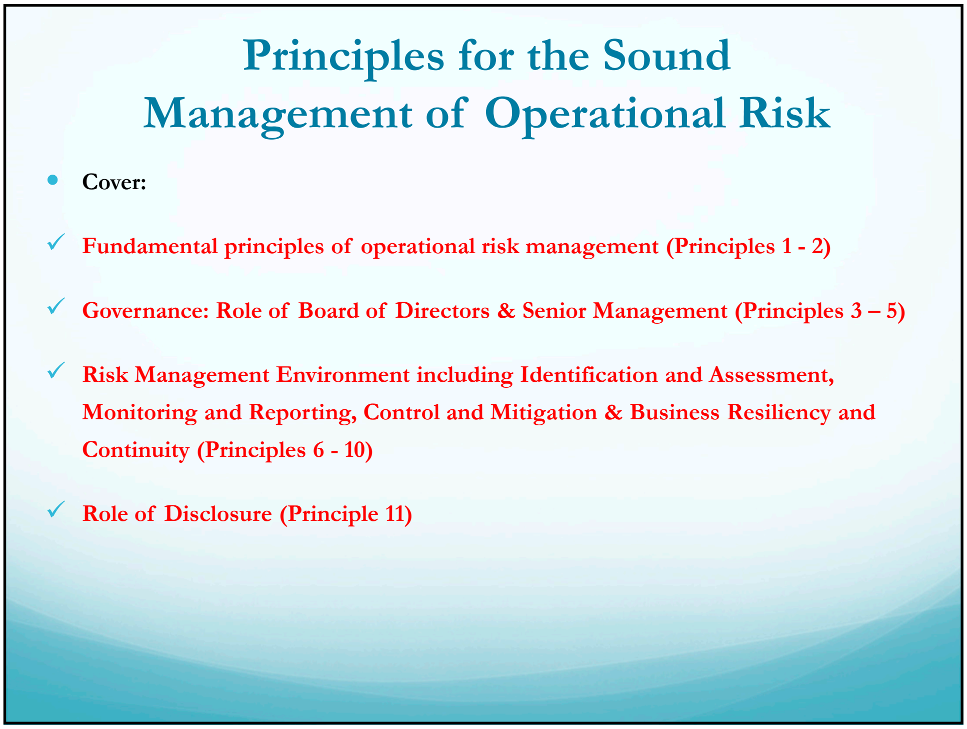


Basel Perspectives: Core Principles

- Basel Core Principle 25: Operational Risk
  - ✓ The supervisor determines that banks have **an adequate operational risk management framework** **that takes into account their risk appetite, risk profile and market and macroeconomic conditions**…..
- Essential Criteria
  - ✓ 4. The supervisor **reviews the quality and comprehensiveness of the bank's disaster recovery and business continuity plans** to assess their feasibility in scenarios of severe business disruption which might plausibly affect the bank……
  - ✓ 5. The supervisor determines that banks **have established appropriate information technology policies and processes to identify, assess, monitor and manage technology risks.** The supervisor also determines that banks have **appropriate and sound information technology infrastructure to meet their current and projected business requirements** ……which ensures **data and system integrity, security and availability and supports integrated and comprehensive risk management.**
  - ✓ 8. The supervisor determines that banks have **established appropriate policies and processes to assess, manage and monitor outsourced activities**……Outsourcing policies and processes **require the bank to have comprehensive contracts and/or service level agreements with a clear allocation of responsibilities** between the outsourcing provider and the bank.

Basel: Principles for Sound Management of Operational Risks (2011)

- Originally developed as 'Sound Practices' by the Basel Committee on Banking Supervision in 2003;
- Revised & enhanced based on lessons learnt from Basel II experiences on operational risk management frameworks in banks;
- **Principles for the Sound Management of Operational Risk** (2011) – now incorporates the evolution of sound practices and details **eleven principles of sound operational risk management covering (1) governance, (2) risk management environment and (3) the role of disclosure.**
- These principles establish sound practices relevant to **all** banks; and when implementing these principles, a bank will take account of the nature, size, complexity and risk profile of its activities.



Principles for the Sound Management of Operational Risk

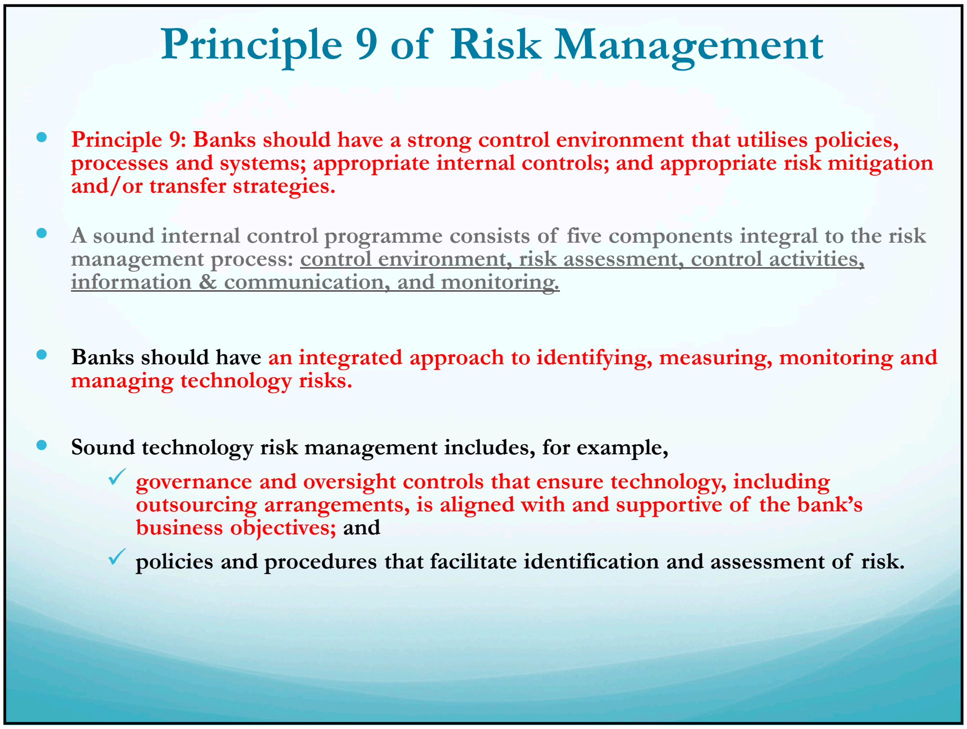
- **Cover:**

✓ **Fundamental principles of operational risk management (Principles 1 - 2)**

✓ **Governance: Role of Board of Directors & Senior Management (Principles 3 – 5)**

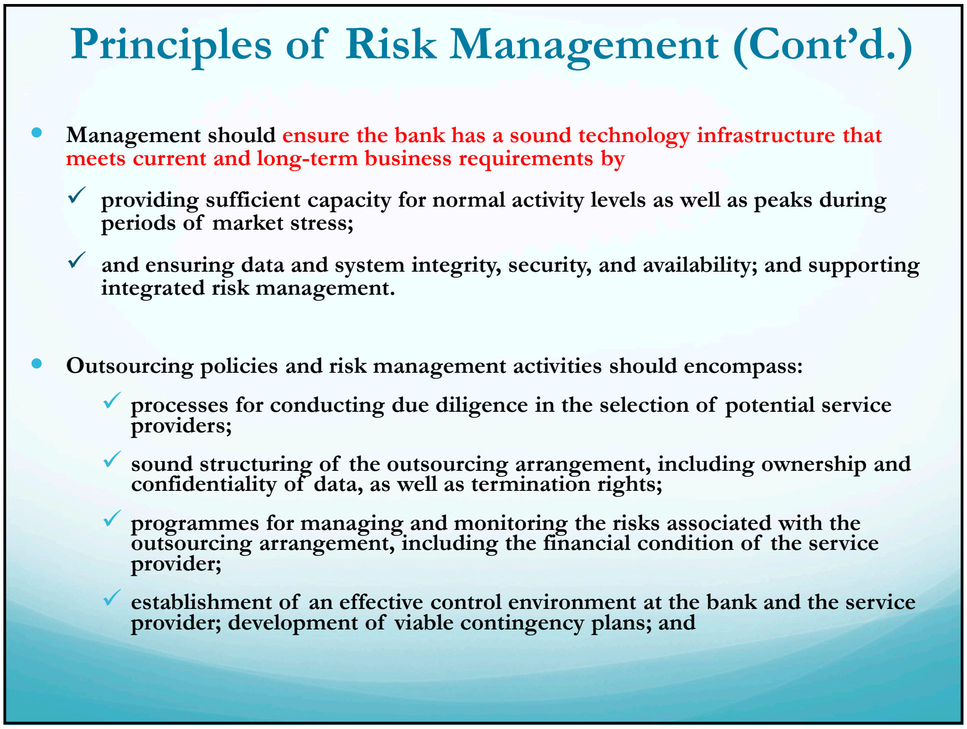
✓ **Risk Management Environment including Identification and Assessment, Monitoring and Reporting, Control and Mitigation & Business Resiliency and Continuity (Principles 6 - 10)**

✓ **Role of Disclosure (Principle 11)**



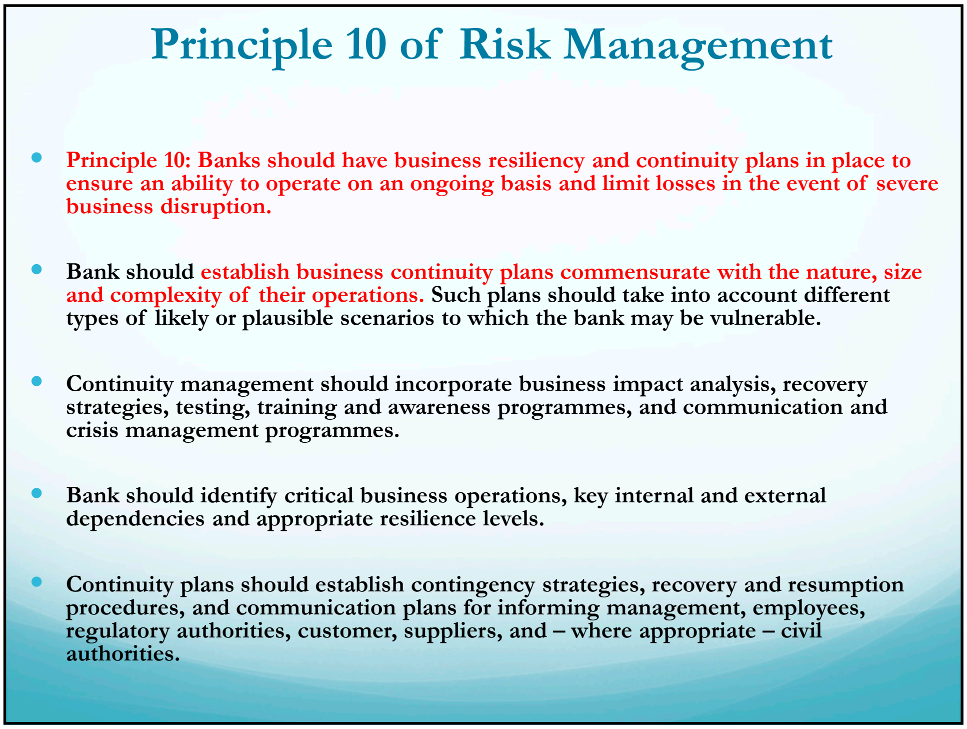
Principle 9 of Risk Management

- Principle 9: Banks should have a strong control environment that utilises policies, processes and systems; appropriate internal controls; and appropriate risk mitigation and/or transfer strategies.
- A sound internal control programme consists of five components integral to the risk management process: control environment, risk assessment, control activities, information & communication, and monitoring.
- Banks should have an integrated approach to identifying, measuring, monitoring and managing technology risks.
- Sound technology risk management includes, for example,
  - ✓ governance and oversight controls that ensure technology, including outsourcing arrangements, is aligned with and supportive of the bank's business objectives; and
  - ✓ policies and procedures that facilitate identification and assessment of risk.



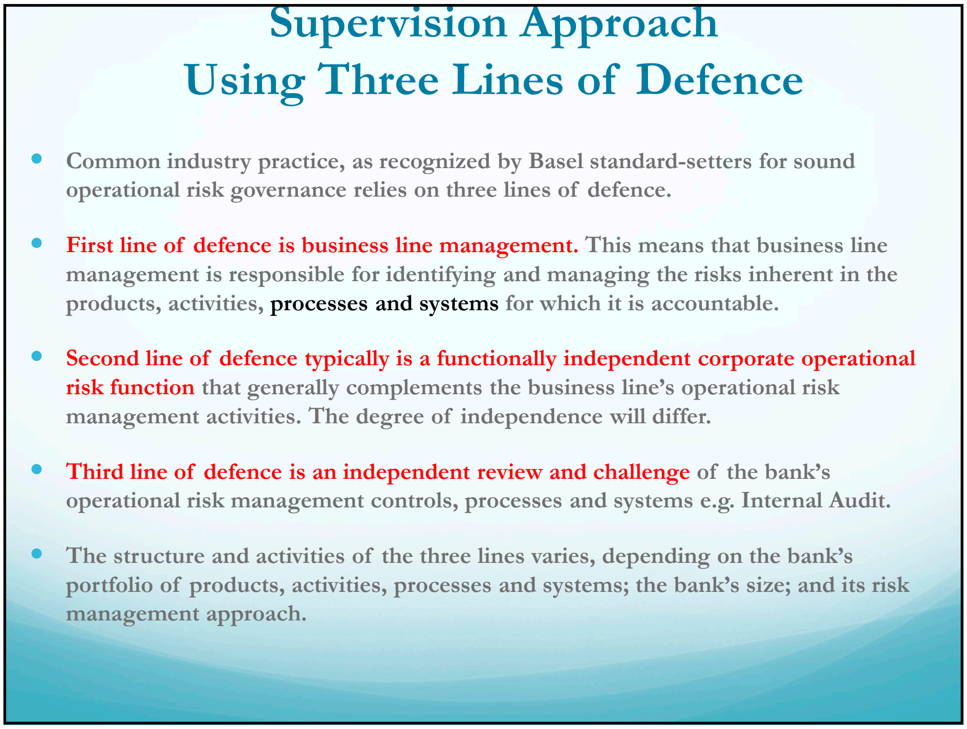
Principles of Risk Management (Cont'd.)

- Management should ensure the bank has a sound technology infrastructure that meets current and long-term business requirements by
  - ✓ providing sufficient capacity for normal activity levels as well as peaks during periods of market stress;
  - ✓ and ensuring data and system integrity, security, and availability; and supporting integrated risk management.
- Outsourcing policies and risk management activities should encompass:
  - ✓ processes for conducting due diligence in the selection of potential service providers;
  - ✓ sound structuring of the outsourcing arrangement, including ownership and confidentiality of data, as well as termination rights;
  - ✓ programmes for managing and monitoring the risks associated with the outsourcing arrangement, including the financial condition of the service provider;
  - ✓ establishment of an effective control environment at the bank and the service provider; development of viable contingency plans; and



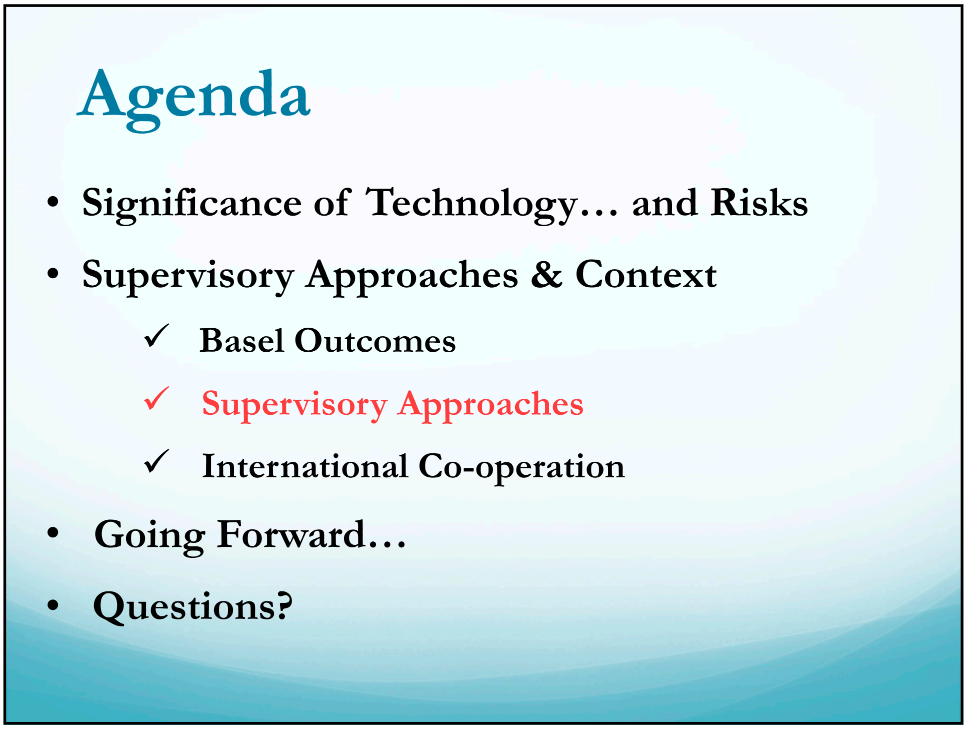
Principle 10 of Risk Management

- Principle 10: Banks should have business resiliency and continuity plans in place to ensure an ability to operate on an ongoing basis and limit losses in the event of severe business disruption.
- Bank should establish business continuity plans commensurate with the nature, size and complexity of their operations. Such plans should take into account different types of likely or plausible scenarios to which the bank may be vulnerable.
- Continuity management should incorporate business impact analysis, recovery strategies, testing, training and awareness programmes, and communication and crisis management programmes.
- Bank should identify critical business operations, key internal and external dependencies and appropriate resilience levels.
- Continuity plans should establish contingency strategies, recovery and resumption procedures, and communication plans for informing management, employees, regulatory authorities, customer, suppliers, and – where appropriate – civil authorities.



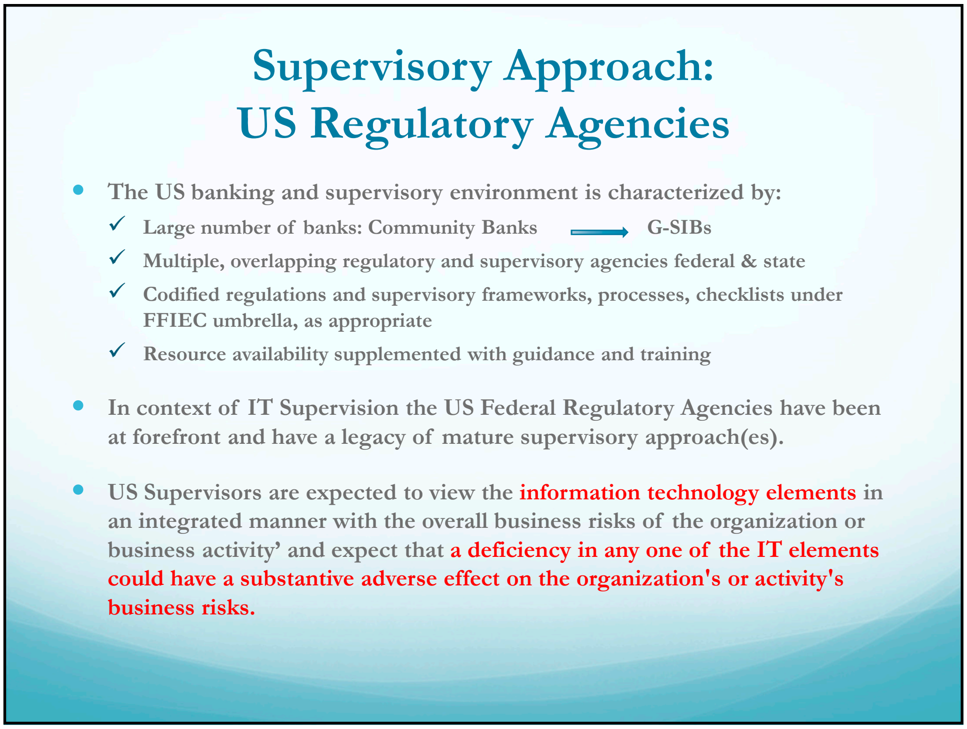
Supervision Approach Using Three Lines of Defence

- Common industry practice, as recognized by Basel standard-setters for sound operational risk governance relies on three lines of defence.
- First line of defence is business line management. This means that business line management is responsible for identifying and managing the risks inherent in the products, activities, processes and systems for which it is accountable.
- Second line of defence typically is a functionally independent corporate operational risk function that generally complements the business line's operational risk management activities. The degree of independence will differ.
- Third line of defence is an independent review and challenge of the bank's operational risk management controls, processes and systems e.g. Internal Audit.
- The structure and activities of the three lines varies, depending on the bank's portfolio of products, activities, processes and systems; the bank's size; and its risk management approach.



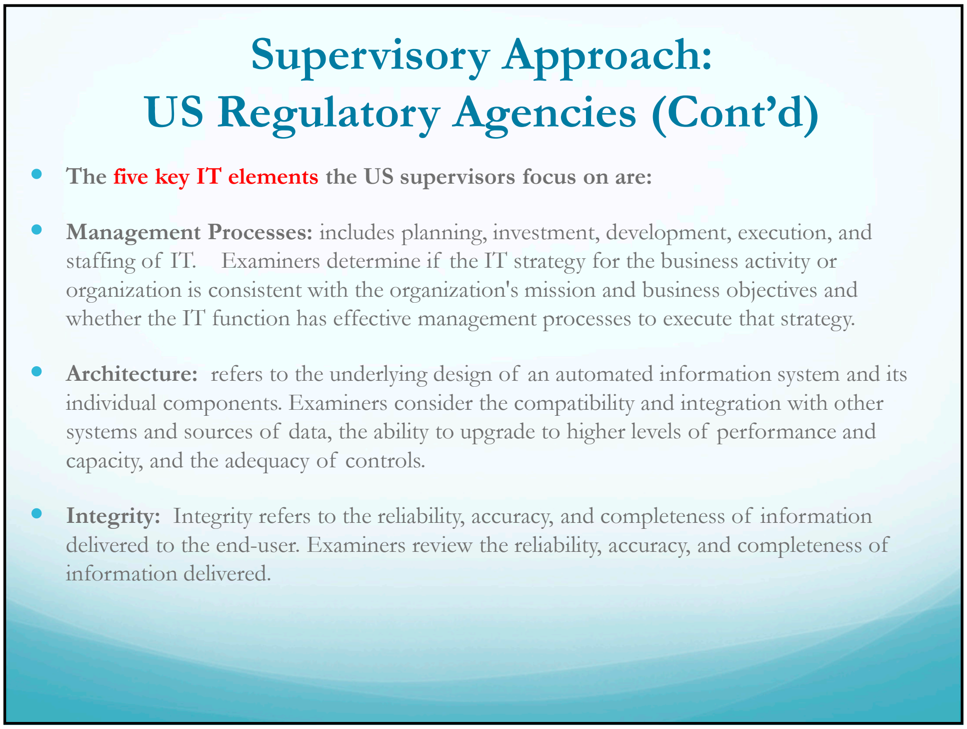
Agenda

- Significance of Technology… and Risks
- Supervisory Approaches & Context
  - ✓ Basel Outcomes
  - ✓ Supervisory Approaches
  - ✓ International Co-operation
- Going Forward…
- Questions?



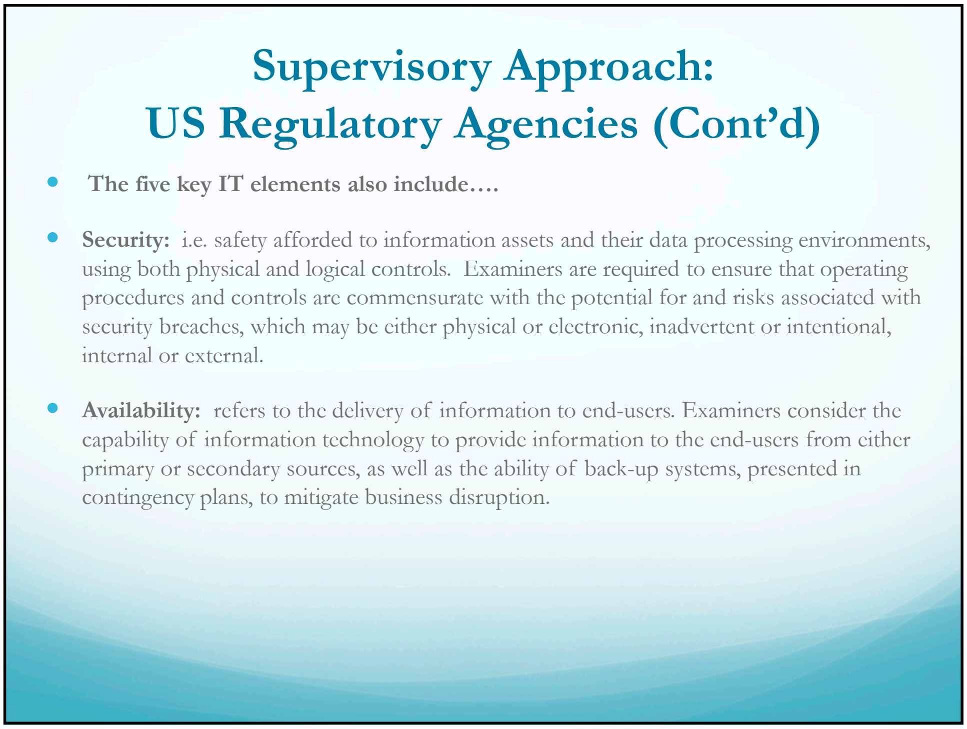
Supervisory Approach: US Regulatory Agencies

- The US banking and supervisory environment is characterized by:
  - ✓ Large number of banks: Community Banks → G-SIBs
  - ✓ Multiple, overlapping regulatory and supervisory agencies federal & state
  - ✓ Codified regulations and supervisory frameworks, processes, checklists under FFIEC umbrella, as appropriate
  - ✓ Resource availability supplemented with guidance and training
- In context of IT Supervision the US Federal Regulatory Agencies have been at forefront and have a legacy of mature supervisory approach(es).
- US Supervisors are expected to view the information technology elements in an integrated manner with the overall business risks of the organization or business activity' and expect that a deficiency in any one of the IT elements could have a substantive adverse effect on the organization's or activity's business risks.



Supervisory Approach: US Regulatory Agencies (Cont'd)

- **The five key IT elements the US supervisors focus on are:**
- **Management Processes:** includes planning, investment, development, execution, and staffing of IT. Examiners determine if the IT strategy for the business activity or organization is consistent with the organization's mission and business objectives and whether the IT function has effective management processes to execute that strategy.
- **Architecture:** refers to the underlying design of an automated information system and its individual components. Examiners consider the compatibility and integration with other systems and sources of data, the ability to upgrade to higher levels of performance and capacity, and the adequacy of controls.
- **Integrity:** Integrity refers to the reliability, accuracy, and completeness of information delivered to the end-user. Examiners review the reliability, accuracy, and completeness of information delivered.



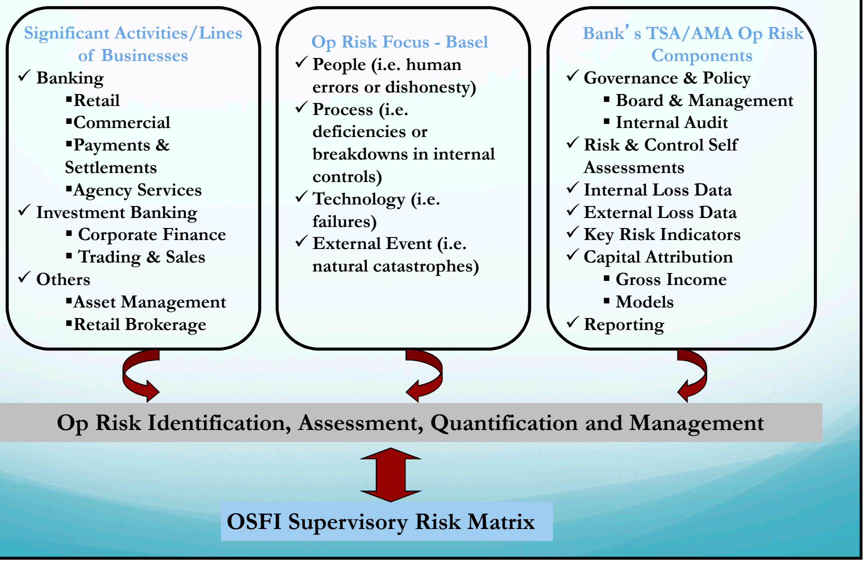
Supervisory Approach: US Regulatory Agencies (Cont'd)

- **The five key IT elements also include….**
- **Security:** i.e. safety afforded to information assets and their data processing environments, using both physical and logical controls. Examiners are required to ensure that operating procedures and controls are commensurate with the potential for and risks associated with security breaches, which may be either physical or electronic, inadvertent or intentional, internal or external.
- **Availability:** refers to the delivery of information to end-users. Examiners consider the capability of information technology to provide information to the end-users from either primary or secondary sources, as well as the ability of back-up systems, presented in contingency plans, to mitigate business disruption.

Supervisory Approach: FFIEC - Resources

- The Federal Financial Institution Examination Council (FFIEC) is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions.
- One of the best resources on IT supervision is the FFIEC Examiner Education Office created the FFIEC InfoBase. The InfoBase provides a wide range of introductory, reference, and educational training material on specific topics of interest to supervisors. (Check out: http://ithandbook.ffiec.gov)
- The US agencies use "Uniform Rating System for Information Technology (URSIT)" to uniformly assess and rate IT-related risks of financial institutions and their service providers. The URSIT is based on a risk evaluation of four critical components: Audit, Management, Development and Acquisition, and Support and Delivery.
- The overall performance of IT within a financial institution or a third-party service provider is reflected by a composite rating. The assigned rating determines the degree of supervisory attention necessary.

Supervisory Approach: OSFI (Canada) Operational & Technology Risk



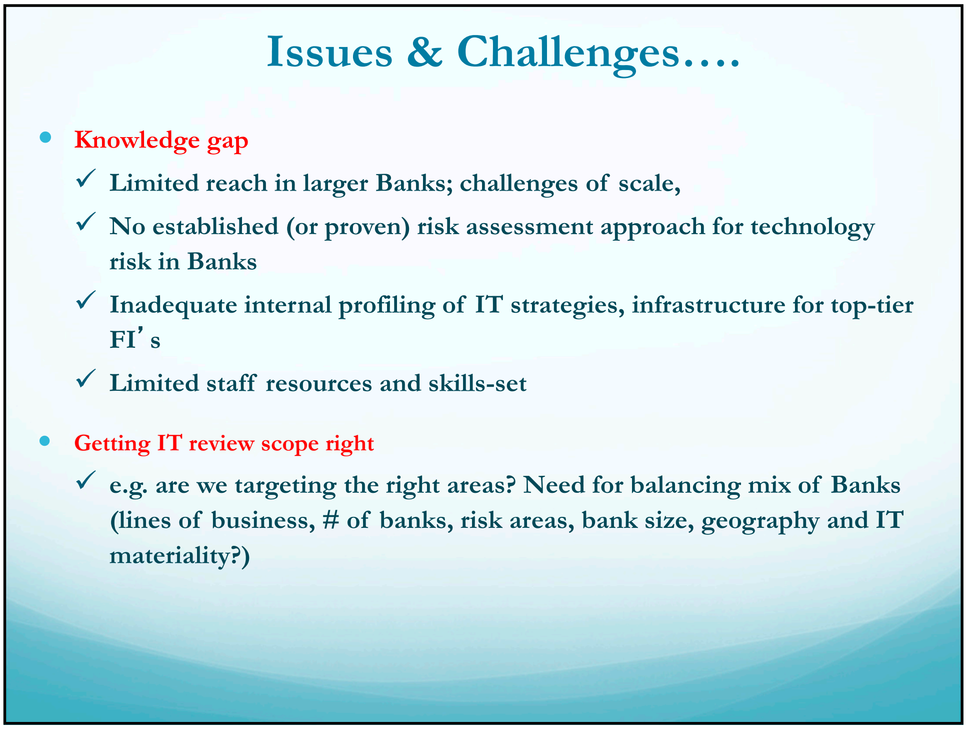
Significant Activities/Lines of Businesses
- ✓ Banking
  - ▪Retail
  - ▪Commercial
  - ▪Payments & Settlements
  - ▪Agency Services
- ✓ Investment Banking
  - ▪ Corporate Finance
  - ▪ Trading & Sales
- ✓ Others
  - ▪Asset Management
  - ▪Retail Brokerage

Op Risk Focus - Basel
- ✓ People (i.e. human errors or dishonesty)
- ✓ Process (i.e. deficiencies or breakdowns in internal controls)
- ✓ Technology (i.e. failures)
- ✓ External Event (i.e. natural catastrophes)

Bank's TSA/AMA Op Risk Components
- ✓ Governance & Policy
  - ▪ Board & Management
  - ▪ Internal Audit
- ✓ Risk & Control Self Assessments
- ✓ Internal Loss Data
- ✓ External Loss Data
- ✓ Key Risk Indicators
- ✓ Capital Attribution
  - ▪ Gross Income
  - ▪ Models
- ✓ Reporting

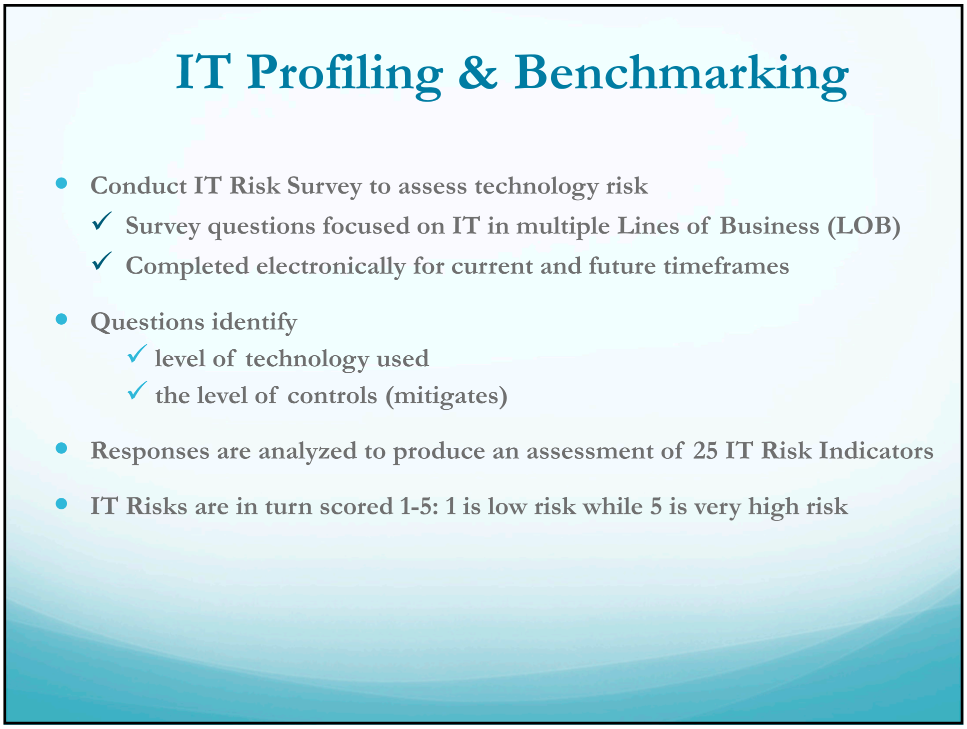
Op Risk Identification, Assessment, Quantification and Management

OSFI Supervisory Risk Matrix



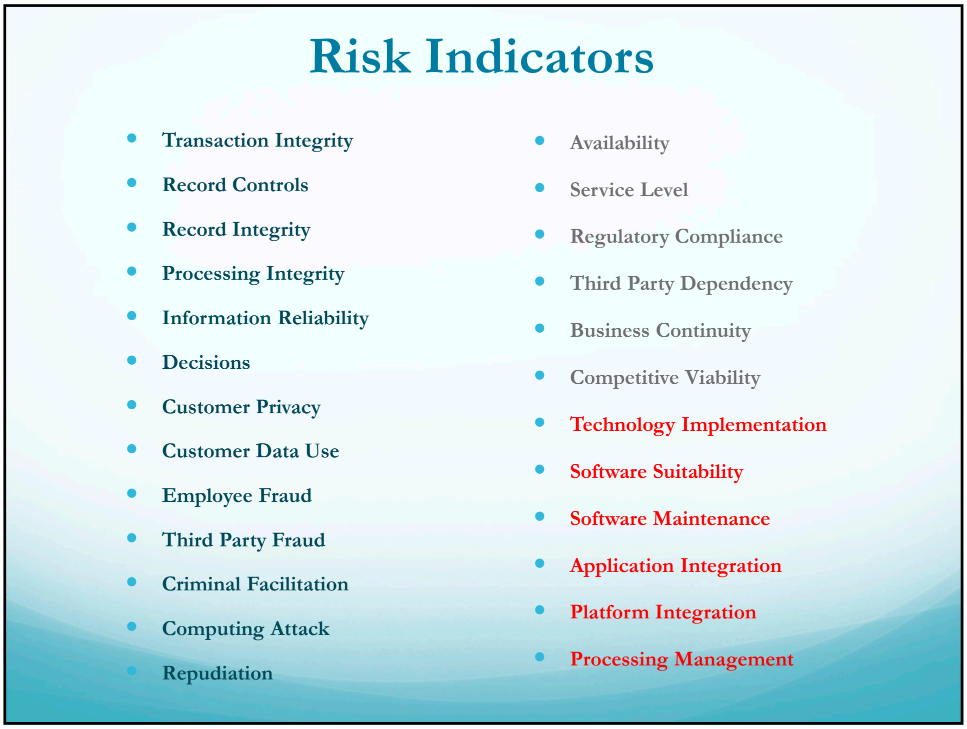
Issues & Challenges….

- Knowledge gap
  - ✓ Limited reach in larger Banks; challenges of scale,
  - ✓ No established (or proven) risk assessment approach for technology risk in Banks
  - ✓ Inadequate internal profiling of IT strategies, infrastructure for top-tier FI's
  - ✓ Limited staff resources and skills-set
- Getting IT review scope right
  - ✓ e.g. are we targeting the right areas? Need for balancing mix of Banks (lines of business, # of banks, risk areas, bank size, geography and IT materiality?)



IT Profiling & Benchmarking

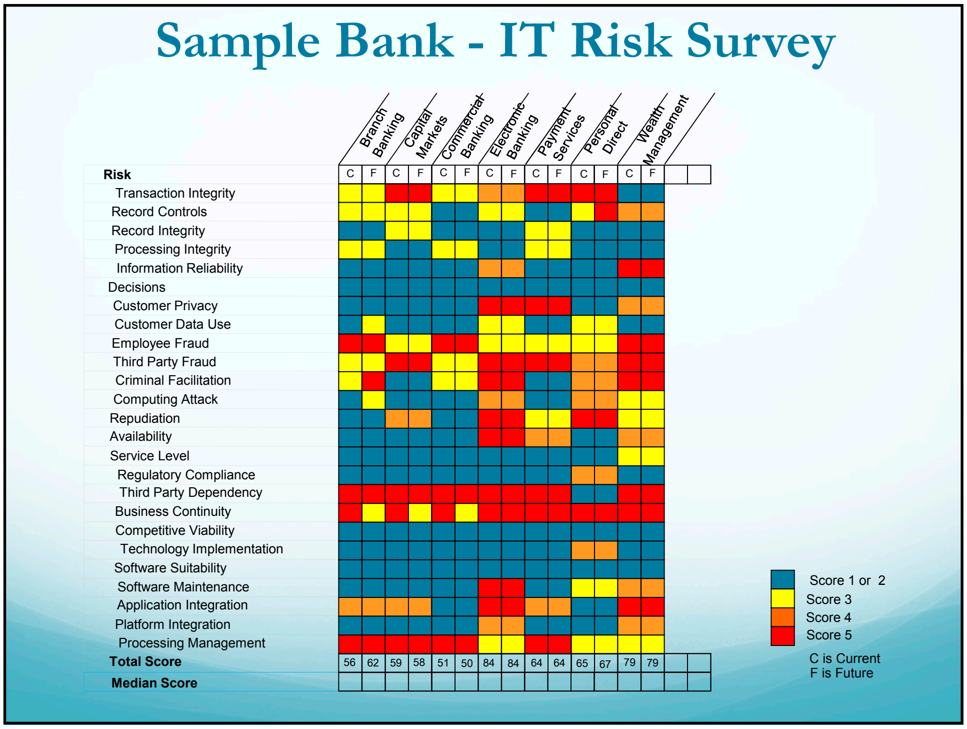
- Conduct IT Risk Survey to assess technology risk
  - ✓ Survey questions focused on IT in multiple Lines of Business (LOB)
  - ✓ Completed electronically for current and future timeframes
- Questions identify
  - ✓ level of technology used
  - ✓ the level of controls (mitigates)
- Responses are analyzed to produce an assessment of 25 IT Risk Indicators
- IT Risks are in turn scored 1-5: 1 is low risk while 5 is very high risk



Risk Indicators

- Transaction Integrity
- Record Controls
- Record Integrity
- Processing Integrity
- Information Reliability
- Decisions
- Customer Privacy
- Customer Data Use
- Employee Fraud
- Third Party Fraud
- Criminal Facilitation
- Computing Attack
- Repudiation

- Availability
- Service Level
- Regulatory Compliance
- Third Party Dependency
- Business Continuity
- Competitive Viability
- Technology Implementation
- Software Suitability
- Software Maintenance
- Application Integration
- Platform Integration
- Processing Management

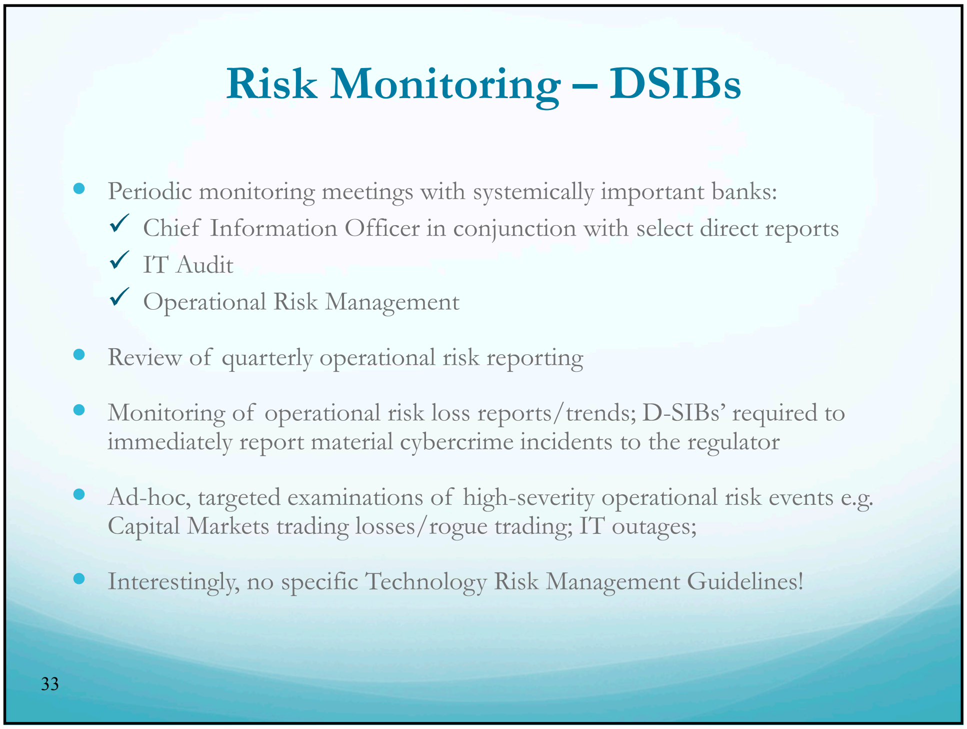


Sample Bank - IT Risk Survey

	Branch Banking		Capital Markets		Commercial Banking		Electronic Banking		Payment Services		Personal Direct		Wealth Management			
Risk	C	F	C	F	C	F	C	F	C	F	C	F	C	F		
Transaction Integrity	🟨	🟨	🟥	🟥	🟨	🟨	🟧	🟧	🟥	🟥	🟥	🟥	🟦	🟦		
Record Controls	🟨	🟨	🟨	🟨	🟦	🟦	🟨	🟨	🟦	🟦	🟨	🟥	🟧	🟧		
Record Integrity	🟦	🟦	🟨	🟨	🟦	🟦	🟦	🟦	🟨	🟨	🟦	🟦	🟦	🟦		
Processing Integrity	🟨	🟨	🟦	🟦	🟨	🟨	🟦	🟦	🟨	🟨	🟦	🟦	🟦	🟦		
Information Reliability	🟦	🟦	🟦	🟦	🟦	🟦	🟧	🟧	🟦	🟦	🟦	🟦	🟥	🟥		
Decisions	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦		
Customer Privacy	🟦	🟦	🟦	🟦	🟦	🟦	🟥	🟥	🟥	🟥	🟦	🟦	🟧	🟧		
Customer Data Use	🟦	🟨	🟦	🟦	🟦	🟦	🟨	🟨	🟦	🟦	🟨	🟨	🟦	🟦		
Employee Fraud	🟥	🟥	🟨	🟨	🟥	🟥	🟨	🟨	🟨	🟨	🟨	🟨	🟥	🟥		
Third Party Fraud	🟨	🟨	🟥	🟥	🟨	🟨	🟥	🟥	🟥	🟥	🟧	🟧	🟥	🟥		
Criminal Facilitation	🟨	🟥	🟦	🟦	🟨	🟨	🟥	🟥	🟦	🟦	🟧	🟧	🟥	🟥		
Computing Attack	🟦	🟨	🟦	🟦	🟦	🟦	🟧	🟧	🟦	🟦	🟧	🟧	🟨	🟨		
Repudiation	🟦	🟦	🟧	🟧	🟦	🟦	🟥	🟥	🟨	🟨	🟥	🟥	🟨	🟨		
Availability	🟦	🟦	🟦	🟦	🟦	🟦	🟥	🟥	🟧	🟧	🟦	🟦	🟧	🟧		
Service Level	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟨	🟨		
Regulatory Compliance	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟧	🟧	🟦	🟦		
Third Party Dependency	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟦	🟦	🟥	🟥		
Business Continuity	🟥	🟨	🟥	🟨	🟥	🟨	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥		
Competitive Viability	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦		
Technology Implementation	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟧	🟧	🟦	🟦		
Software Suitability	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦		
Software Maintenance	🟦	🟦	🟦	🟦	🟦	🟦	🟥	🟥	🟦	🟦	🟨	🟨	🟧	🟧		
Application Integration	🟧	🟧	🟧	🟧	🟦	🟦	🟥	🟥	🟧	🟧	🟦	🟦	🟥	🟥		
Platform Integration	🟦	🟦	🟦	🟦	🟦	🟦	🟧	🟧	🟦	🟦	🟦	🟦	🟧	🟧		
Processing Management	🟥	🟥	🟥	🟥	🟥	🟥	🟨	🟨	🟥	🟥	🟨	🟨	🟨	🟨		
Total Score	56	62	59	58	51	50	84	84	64	64	65	67	79	79		
Median Score																

🟦 Score 1 or 2
🟨 Score 3
🟧 Score 4
🟥 Score 5

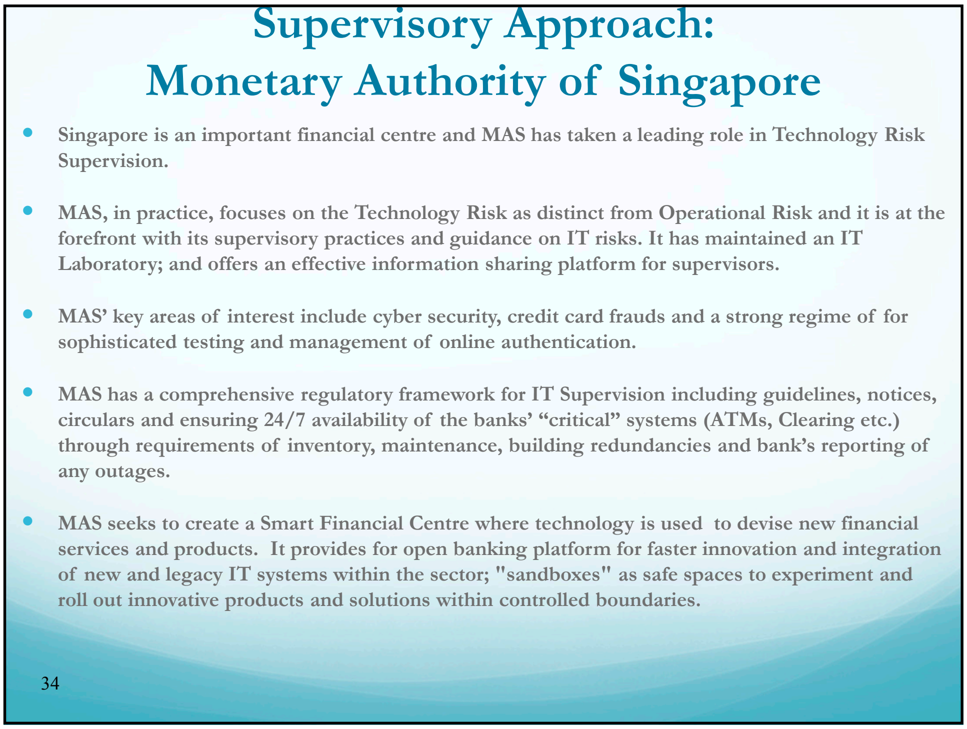
C is Current
F is Future



Risk Monitoring – DSIBs

- Periodic monitoring meetings with systemically important banks:
  - ✓ Chief Information Officer in conjunction with select direct reports
  - ✓ IT Audit
  - ✓ Operational Risk Management
- Review of quarterly operational risk reporting
- Monitoring of operational risk loss reports/trends; D-SIBs' required to immediately report material cybercrime incidents to the regulator
- Ad-hoc, targeted examinations of high-severity operational risk events e.g. Capital Markets trading losses/rogue trading; IT outages;
- Interestingly, no specific Technology Risk Management Guidelines!

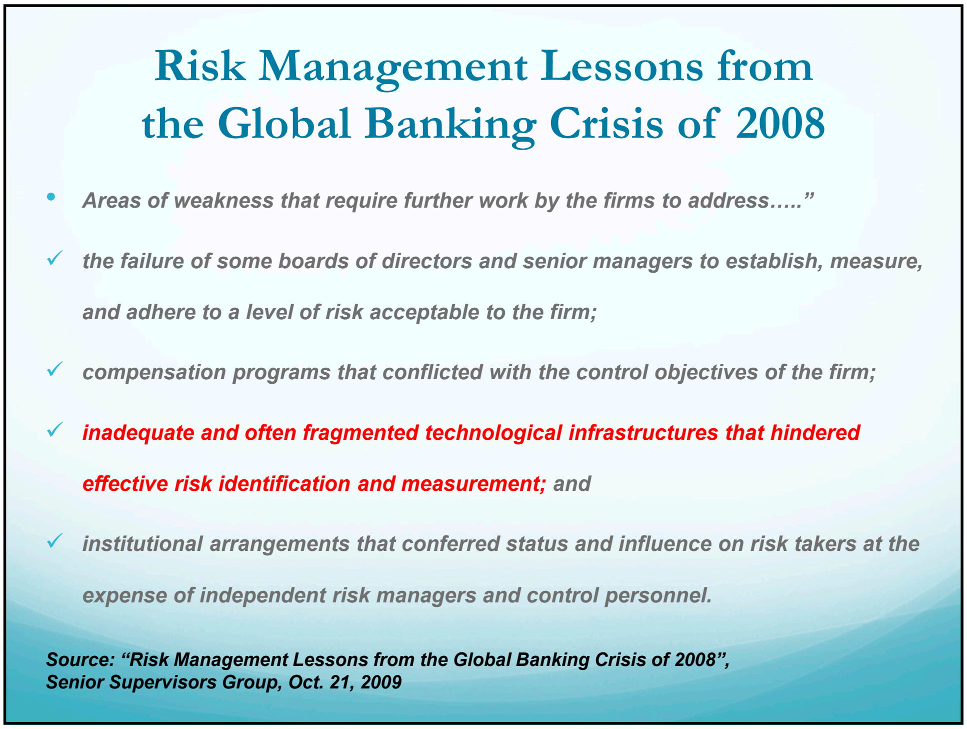
33



Supervisory Approach:
Monetary Authority of Singapore

- **Singapore is an important financial centre and MAS has taken a leading role in Technology Risk Supervision.**
- **MAS, in practice, focuses on the Technology Risk as distinct from Operational Risk and it is at the forefront with its supervisory practices and guidance on IT risks. It has maintained an IT Laboratory; and offers an effective information sharing platform for supervisors.**
- **MAS' key areas of interest include cyber security, credit card frauds and a strong regime of for sophisticated testing and management of online authentication.**
- **MAS has a comprehensive regulatory framework for IT Supervision including guidelines, notices, circulars and ensuring 24/7 availability of the banks' "critical" systems (ATMs, Clearing etc.) through requirements of inventory, maintenance, building redundancies and bank's reporting of any outages.**
- **MAS seeks to create a Smart Financial Centre where technology is used to devise new financial services and products. It provides for open banking platform for faster innovation and integration of new and legacy IT systems within the sector; "sandboxes" as safe spaces to experiment and roll out innovative products and solutions within controlled boundaries.**

34



Risk Management Lessons from the Global Banking Crisis of 2008

- *Areas of weakness that require further work by the firms to address…..”*

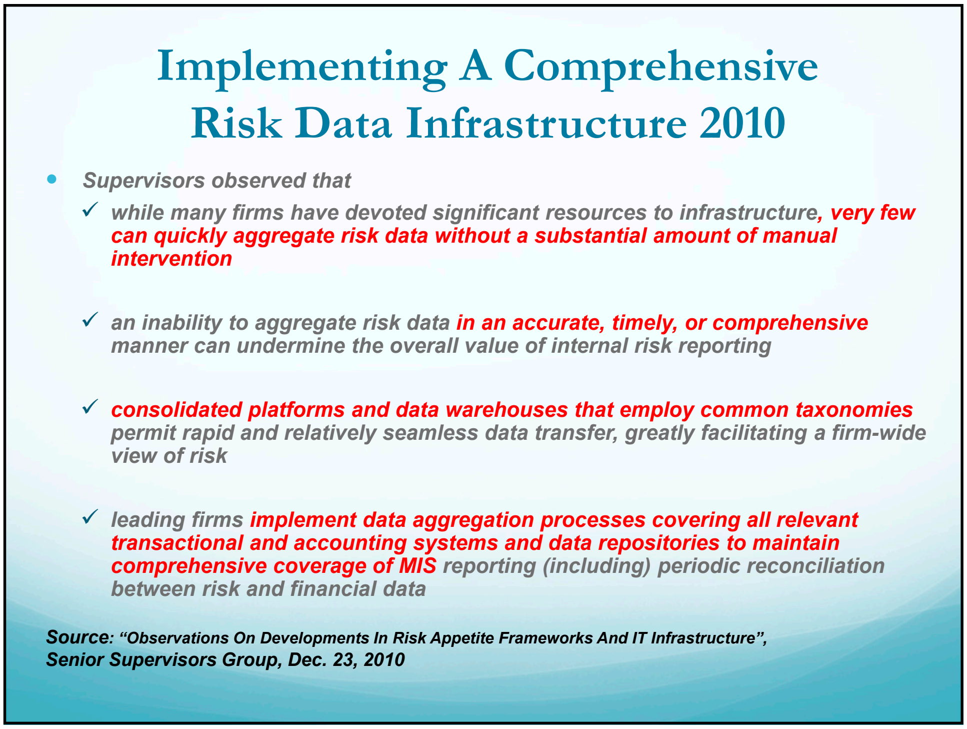
✓ *the failure of some boards of directors and senior managers to establish, measure, and adhere to a level of risk acceptable to the firm;*

✓ *compensation programs that conflicted with the control objectives of the firm;*

✓ ***inadequate and often fragmented technological infrastructures that hindered effective risk identification and measurement;** and*

✓ *institutional arrangements that conferred status and influence on risk takers at the expense of independent risk managers and control personnel.*

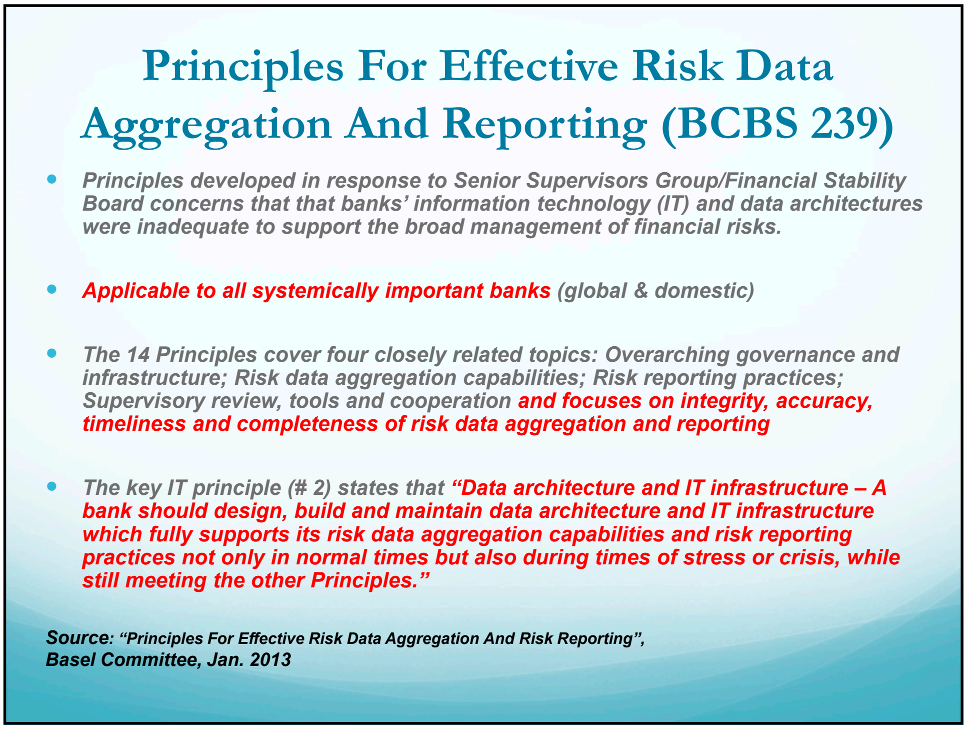
Source: “Risk Management Lessons from the Global Banking Crisis of 2008”,
Senior Supervisors Group, Oct. 21, 2009



Implementing A Comprehensive Risk Data Infrastructure 2010

- *Supervisors observed that*
  - ✓ *while many firms have devoted significant resources to infrastructure**, very few can quickly aggregate risk data without a substantial amount of manual intervention***
  - ✓ *an inability to aggregate risk data **in an accurate, timely, or comprehensive** manner can undermine the overall value of internal risk reporting*
  - ✓ ***consolidated platforms and data warehouses that employ common taxonomies** permit rapid and relatively seamless data transfer, greatly facilitating a firm-wide view of risk*
  - ✓ *leading firms **implement data aggregation processes covering all relevant transactional and accounting systems and data repositories to maintain comprehensive coverage of MIS** reporting (including) periodic reconciliation between risk and financial data*

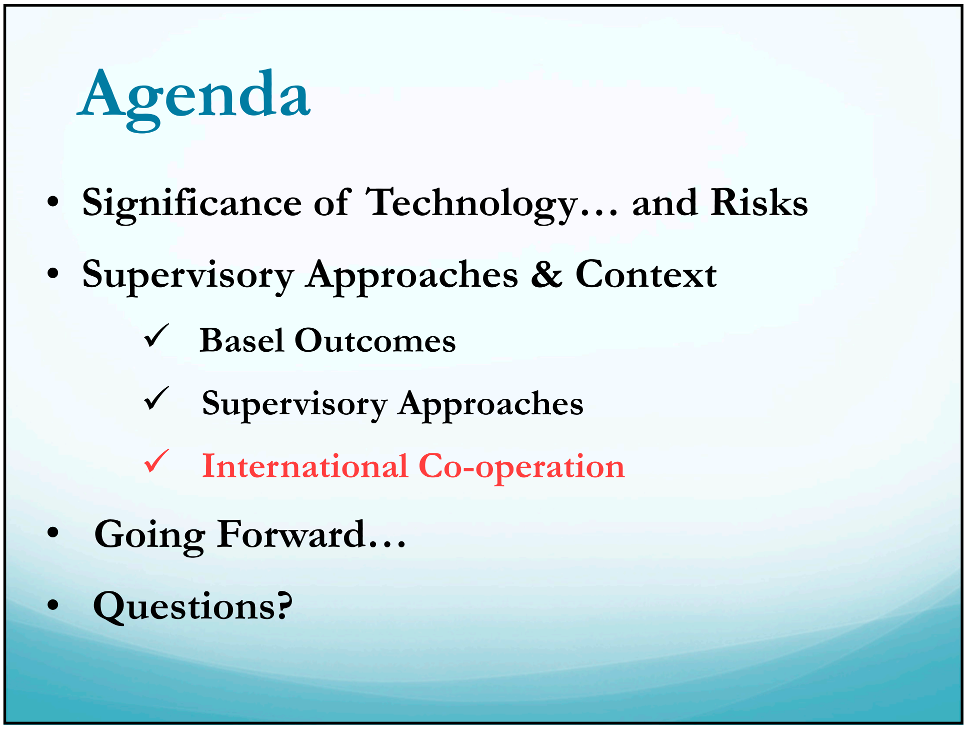
Source: “Observations On Developments In Risk Appetite Frameworks And IT Infrastructure”,
Senior Supervisors Group, Dec. 23, 2010



Principles For Effective Risk Data Aggregation And Reporting (BCBS 239)

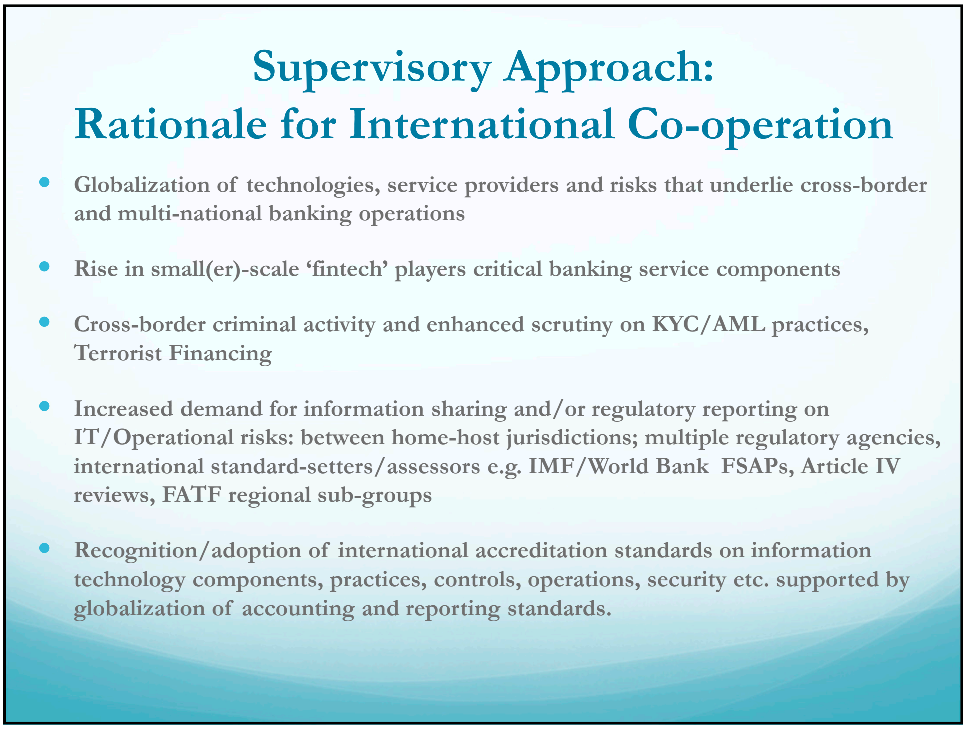
- *Principles developed in response to Senior Supervisors Group/Financial Stability Board concerns that that banks' information technology (IT) and data architectures were inadequate to support the broad management of financial risks.*
- ***Applicable to all systemically important banks*** *(global & domestic)*
- *The 14 Principles cover four closely related topics: Overarching governance and infrastructure; Risk data aggregation capabilities; Risk reporting practices; Supervisory review, tools and cooperation* ***and focuses on integrity, accuracy, timeliness and completeness of risk data aggregation and reporting***
- *The key IT principle (# 2) states that* ***"Data architecture and IT infrastructure – A bank should design, build and maintain data architecture and IT infrastructure which fully supports its risk data aggregation capabilities and risk reporting practices not only in normal times but also during times of stress or crisis, while still meeting the other Principles."***

Source***: "Principles For Effective Risk Data Aggregation And Risk Reporting",***
Basel Committee, Jan. 2013



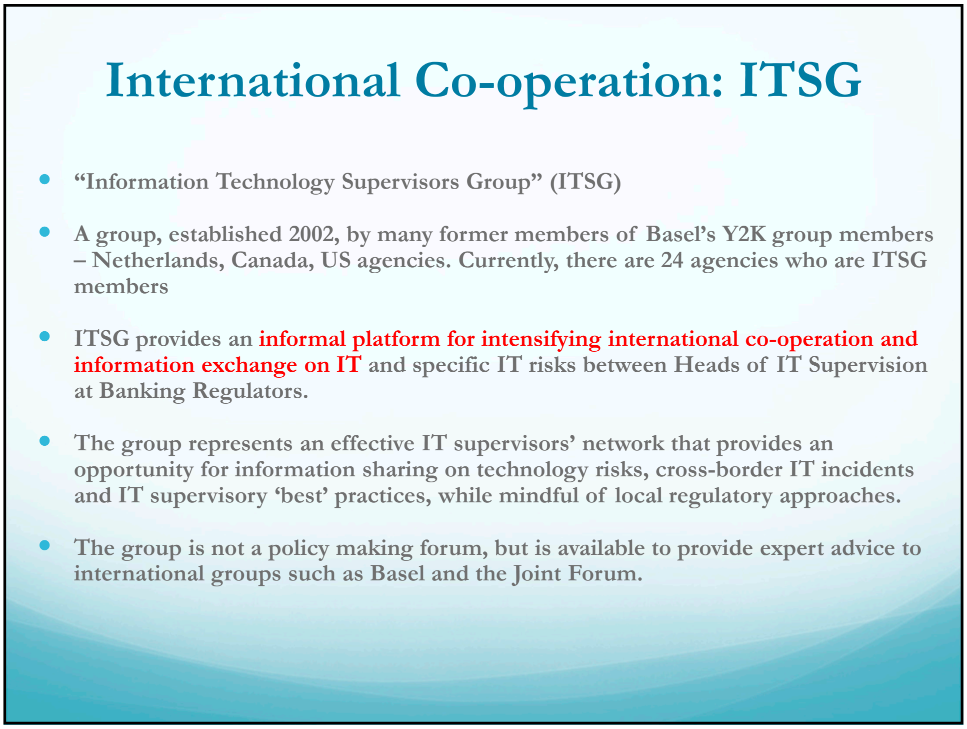
Agenda

- Significance of Technology… and Risks
- Supervisory Approaches & Context
  - ✓ Basel Outcomes
  - ✓ Supervisory Approaches
  - ✓ International Co-operation
- Going Forward…
- Questions?



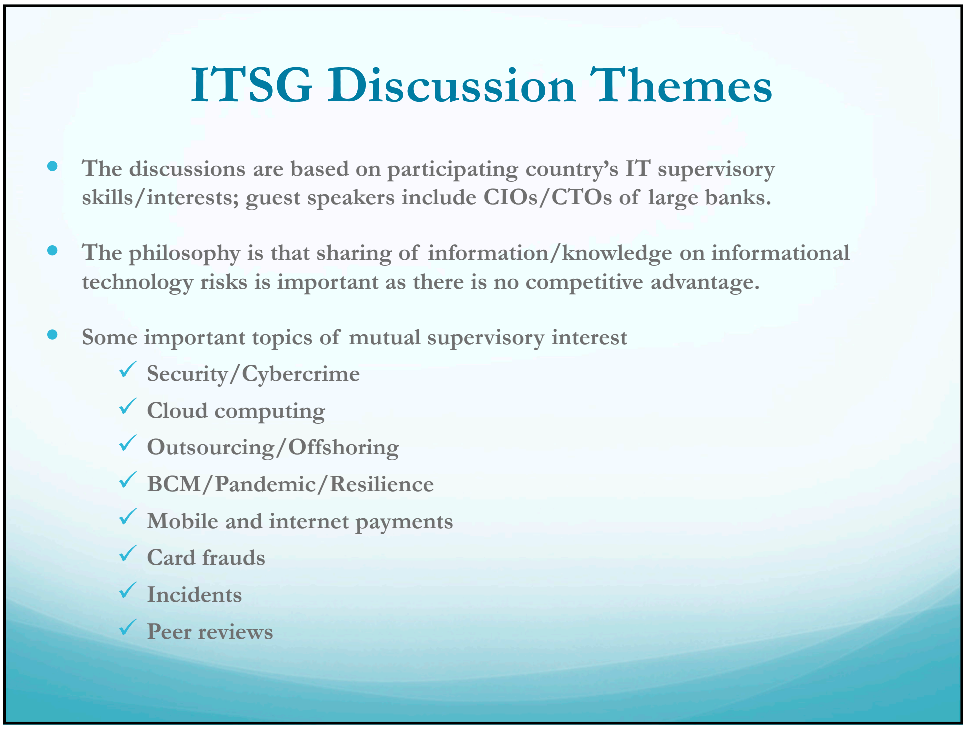
Supervisory Approach: Rationale for International Co-operation

- Globalization of technologies, service providers and risks that underlie cross-border and multi-national banking operations
- Rise in small(er)-scale ‘fintech’ players critical banking service components
- Cross-border criminal activity and enhanced scrutiny on KYC/AML practices, Terrorist Financing
- Increased demand for information sharing and/or regulatory reporting on IT/Operational risks: between home-host jurisdictions; multiple regulatory agencies, international standard-setters/assessors e.g. IMF/World Bank FSAPs, Article IV reviews, FATF regional sub-groups
- Recognition/adoption of international accreditation standards on information technology components, practices, controls, operations, security etc. supported by globalization of accounting and reporting standards.



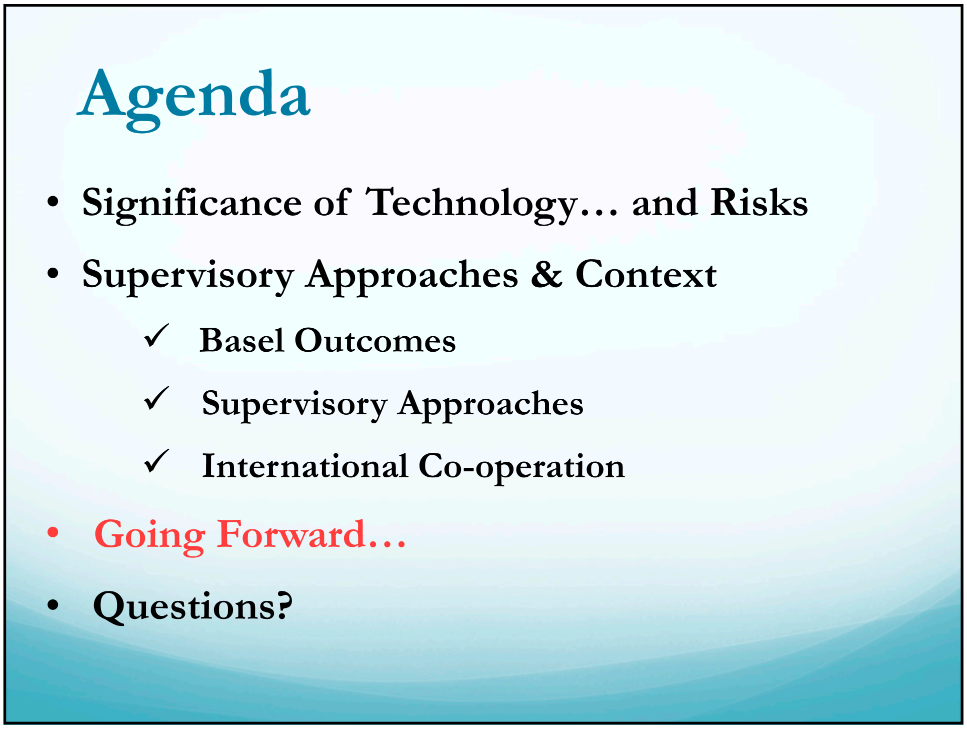
International Co-operation: ITSG

- “Information Technology Supervisors Group” (ITSG)
- A group, established 2002, by many former members of Basel’s Y2K group members – Netherlands, Canada, US agencies. Currently, there are 24 agencies who are ITSG members
- ITSG provides an **informal platform for intensifying international co-operation and information exchange on IT** and specific IT risks between Heads of IT Supervision at Banking Regulators.
- The group represents an effective IT supervisors’ network that provides an opportunity for information sharing on technology risks, cross-border IT incidents and IT supervisory ‘best’ practices, while mindful of local regulatory approaches.
- The group is not a policy making forum, but is available to provide expert advice to international groups such as Basel and the Joint Forum.



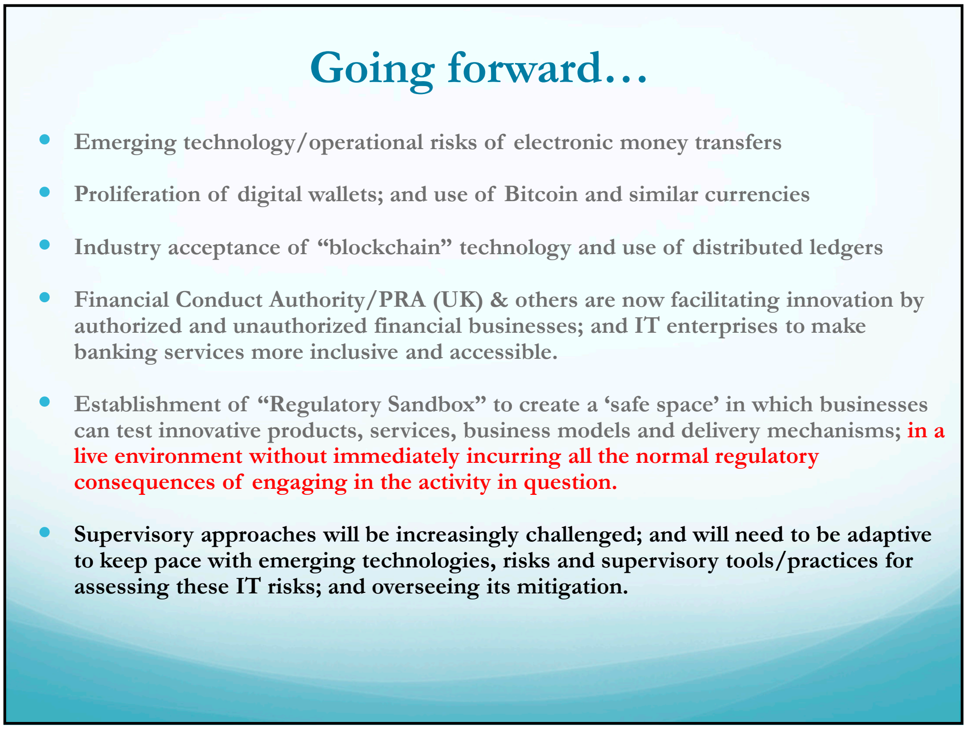
ITSG Discussion Themes

- The discussions are based on participating country’s IT supervisory skills/interests; guest speakers include CIOs/CTOs of large banks.
- The philosophy is that sharing of information/knowledge on informational technology risks is important as there is no competitive advantage.
- Some important topics of mutual supervisory interest
  - ✓ Security/Cybercrime
  - ✓ Cloud computing
  - ✓ Outsourcing/Offshoring
  - ✓ BCM/Pandemic/Resilience
  - ✓ Mobile and internet payments
  - ✓ Card frauds
  - ✓ Incidents
  - ✓ Peer reviews



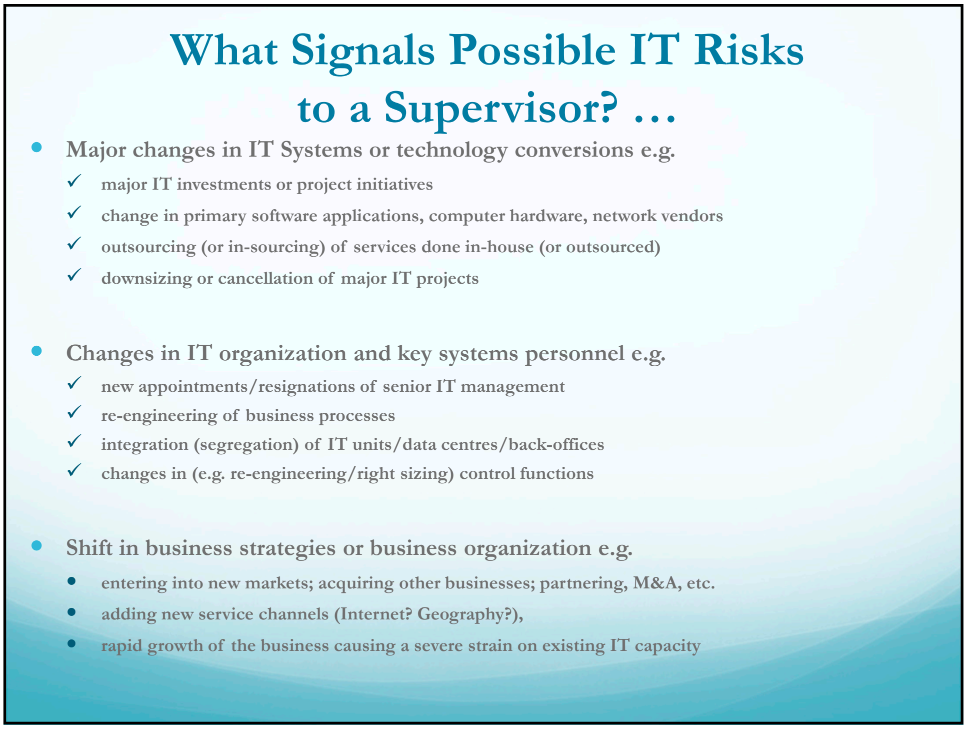
Agenda

- Significance of Technology… and Risks
- Supervisory Approaches & Context
  - ✓ Basel Outcomes
  - ✓ Supervisory Approaches
  - ✓ International Co-operation
- Going Forward…
- Questions?



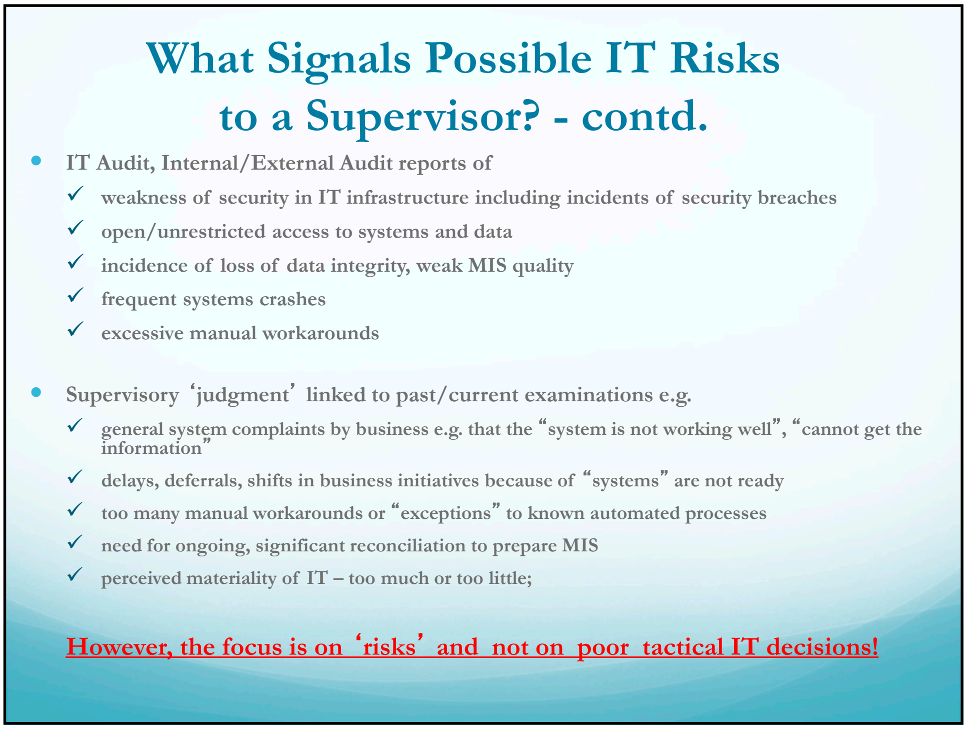
Going forward…

- Emerging technology/operational risks of electronic money transfers
- Proliferation of digital wallets; and use of Bitcoin and similar currencies
- Industry acceptance of "blockchain" technology and use of distributed ledgers
- Financial Conduct Authority/PRA (UK) & others are now facilitating innovation by authorized and unauthorized financial businesses; and IT enterprises to make banking services more inclusive and accessible.
- Establishment of "Regulatory Sandbox" to create a 'safe space' in which businesses can test innovative products, services, business models and delivery mechanisms; in a live environment without immediately incurring all the normal regulatory consequences of engaging in the activity in question.
- **Supervisory approaches will be increasingly challenged; and will need to be adaptive to keep pace with emerging technologies, risks and supervisory tools/practices for assessing these IT risks; and overseeing its mitigation.**



What Signals Possible IT Risks to a Supervisor? …

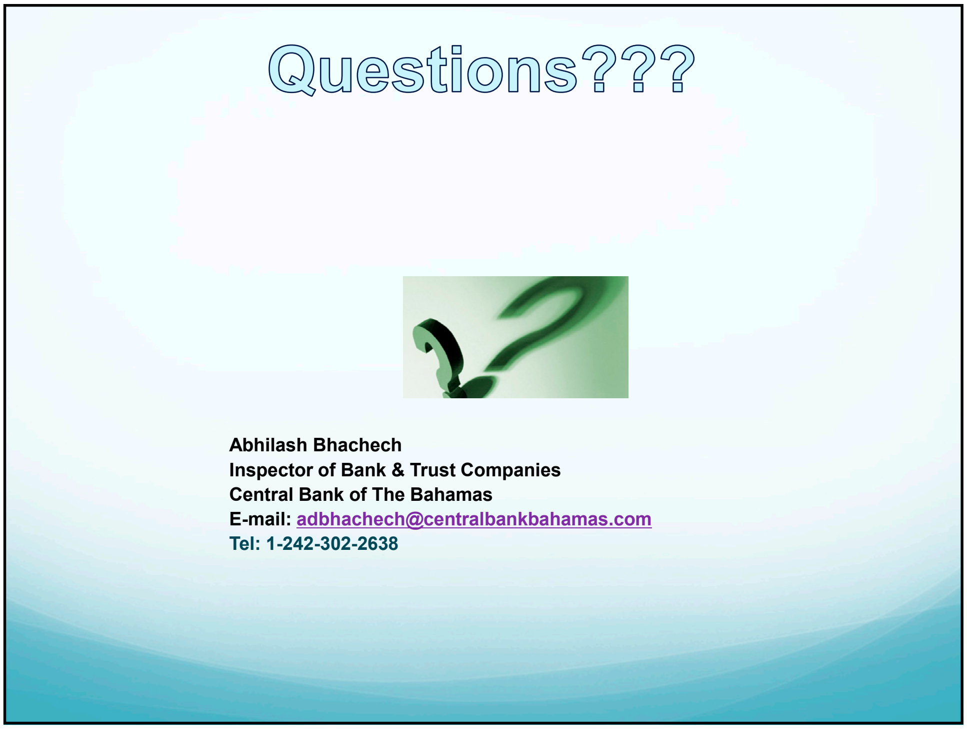
- Major changes in IT Systems or technology conversions e.g.
  - ✓ major IT investments or project initiatives
  - ✓ change in primary software applications, computer hardware, network vendors
  - ✓ outsourcing (or in-sourcing) of services done in-house (or outsourced)
  - ✓ downsizing or cancellation of major IT projects
- Changes in IT organization and key systems personnel e.g.
  - ✓ new appointments/resignations of senior IT management
  - ✓ re-engineering of business processes
  - ✓ integration (segregation) of IT units/data centres/back-offices
  - ✓ changes in (e.g. re-engineering/right sizing) control functions
- Shift in business strategies or business organization e.g.
  - entering into new markets; acquiring other businesses; partnering, M&A, etc.
  - adding new service channels (Internet? Geography?),
  - rapid growth of the business causing a severe strain on existing IT capacity



What Signals Possible IT Risks to a Supervisor? - contd.

- IT Audit, Internal/External Audit reports of
  - ✓ weakness of security in IT infrastructure including incidents of security breaches
  - ✓ open/unrestricted access to systems and data
  - ✓ incidence of loss of data integrity, weak MIS quality
  - ✓ frequent systems crashes
  - ✓ excessive manual workarounds
- Supervisory 'judgment' linked to past/current examinations e.g.
  - ✓ general system complaints by business e.g. that the "system is not working well", "cannot get the information"
  - ✓ delays, deferrals, shifts in business initiatives because of "systems" are not ready
  - ✓ too many manual workarounds or "exceptions" to known automated processes
  - ✓ need for ongoing, significant reconciliation to prepare MIS
  - ✓ perceived materiality of IT – too much or too little;

However, the focus is on 'risks' and not on poor tactical IT decisions!



Questions???

Abhilash Bhachech
Inspector of Bank & Trust Companies
Central Bank of The Bahamas
E-mail: adbhachech@centralbankbahamas.com
Tel: 1-242-302-2638

Regional Approach to Technology Risk Supervision

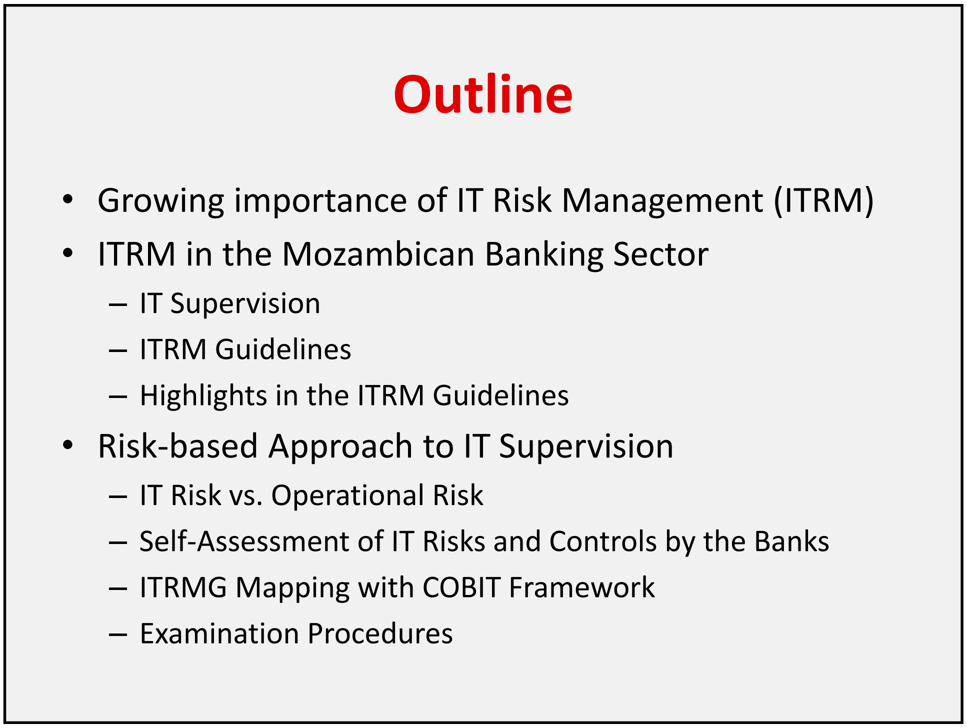
Seminar on Technology Risk Supervision

International Monetary Fund, East AFRITAC

Dar es Salaam, Tanzania

September 15 – 16, 2016

Dércio Mutimucuio
Principal Bank Examiner
Banco de Moçambique

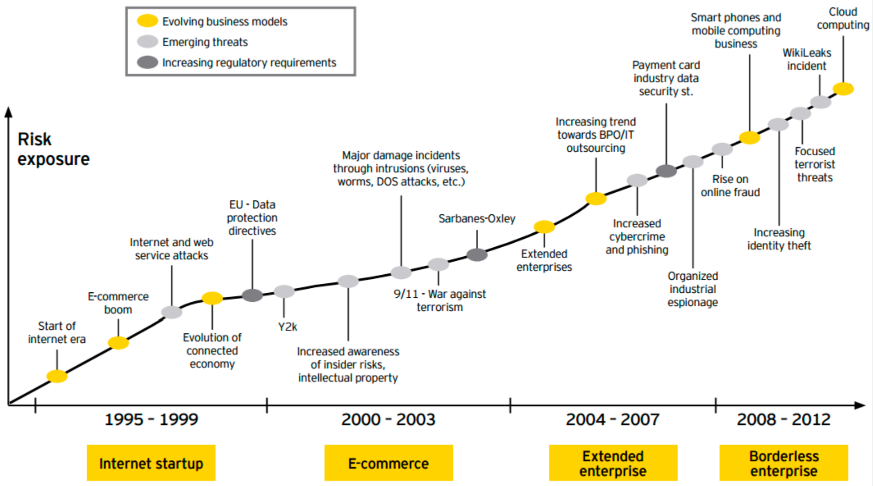


Outline

- Growing importance of IT Risk Management (ITRM)
- ITRM in the Mozambican Banking Sector
  - IT Supervision
  - ITRM Guidelines
  - Highlights in the ITRM Guidelines
- Risk-based Approach to IT Supervision
  - IT Risk vs. Operational Risk
  - Self-Assessment of IT Risks and Controls by the Banks
  - ITRMG Mapping with COBIT Framework
  - Examination Procedures

Growing importance of IT Risk Management (ITRM)

Growing Importance of ITRM



Source: *The Ernst & Young Business Risk Report 2010*. Available at www.ey.com

Growing Importance of ITRM

IT risk is business risk – specifically, the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise.

ITGI (2009)

- The value of IT in a bank depends on the way IS/IT are implemented and related to the banking activities
  - IT represents an important factor of competitiveness

ITRM in the Mozambican Banking Sector

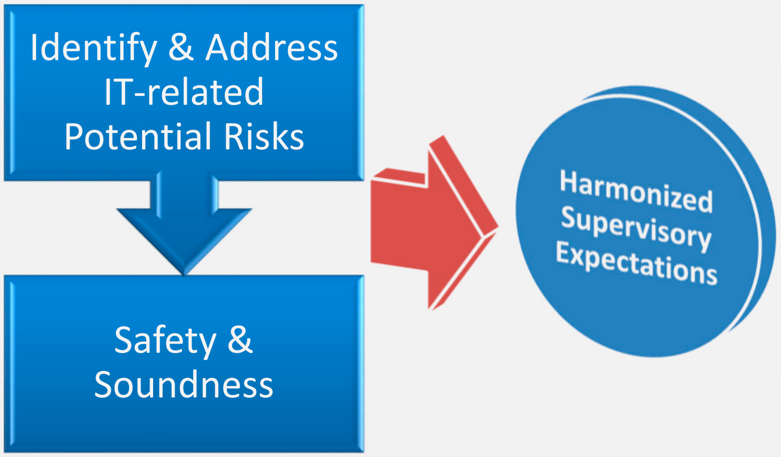
- ***IT Supervision in Mozambique***
- ***ITRM Guidelines in Mozambique***
- ***Highlights in the Guidelines***

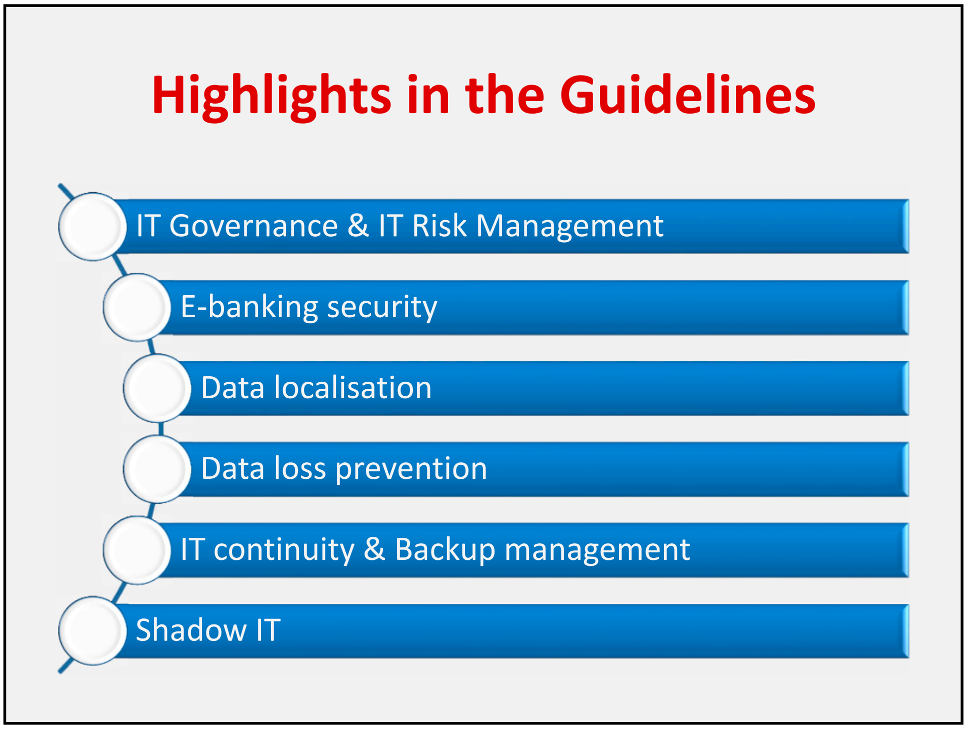
IT Supervision in Mozambique

- Supervision of IT-related risks in Mozambican banks started in 2007
  - COBIT framework and FFIEC Examination Handbooks were used for onsite examinations → *ad hoc approach*
  - Challenges:
    - Discussing the examination findings with banks' management without preset expectations
    - Transmitting the need for ITRM without harmonized supervisory expectation.

ITRM Guidelines in Mozambique

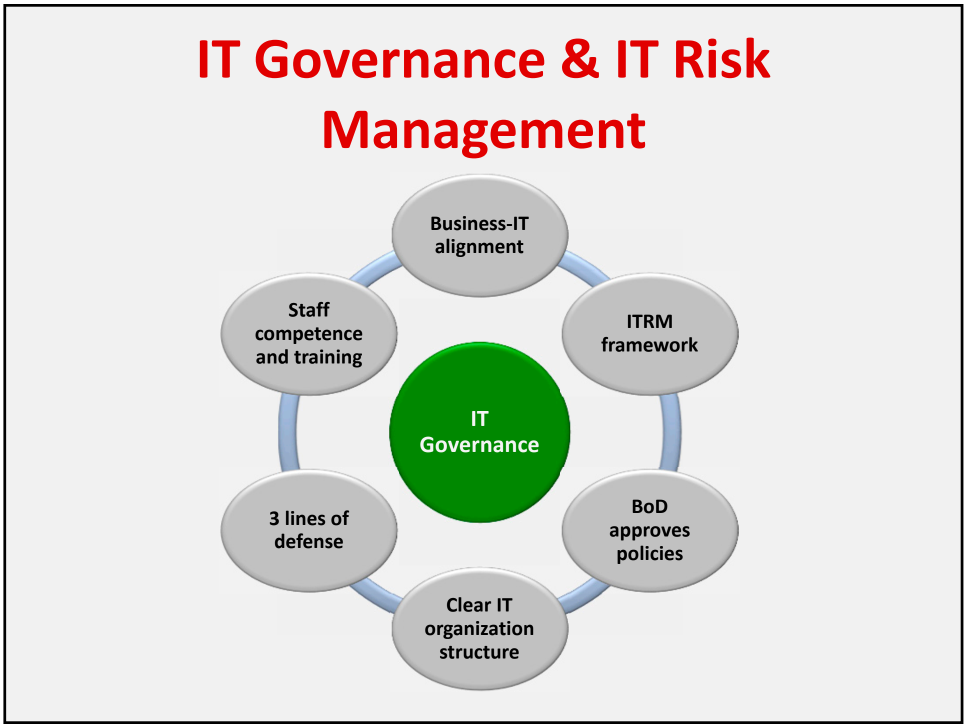
- In 2013, Bank of Mozambique issued its set of ITRM Guidelines (ITRMG):


Identify & Address IT-related Potential Risks
Safety & Soundness
Harmonized Supervisory Expectations



Highlights in the Guidelines

- IT Governance & IT Risk Management
- E-banking security
- Data localisation
- Data loss prevention
- IT continuity & Backup management
- Shadow IT



IT Governance & IT Risk Management

IT Governance

Business-IT alignment

ITRM framework

BoD approves policies

Clear IT organization structure

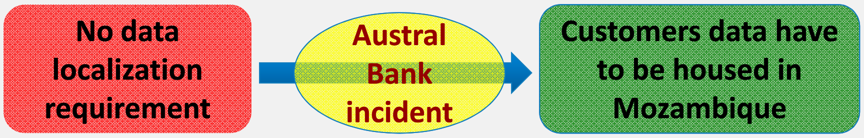
3 lines of defense

Staff competence and training

E-banking security

- Assure users that login access and transactions over the Internet and mobile online services are protected and authenticated
- Adopt well-established encryption algorithms & protection of confidential information used for mobile online payments
- Maintain high resiliency and availability (protection against DoS/ DDoS attacks, MITMA, etc.)
- Establish two-factor authentication at login for internet banking systems
- Transaction signing for authorising transactions
- Ensure payment card data encryption in storage and transmission/ introduce payment cards that comply with EMV standards

Data Localization


No data localization requirement

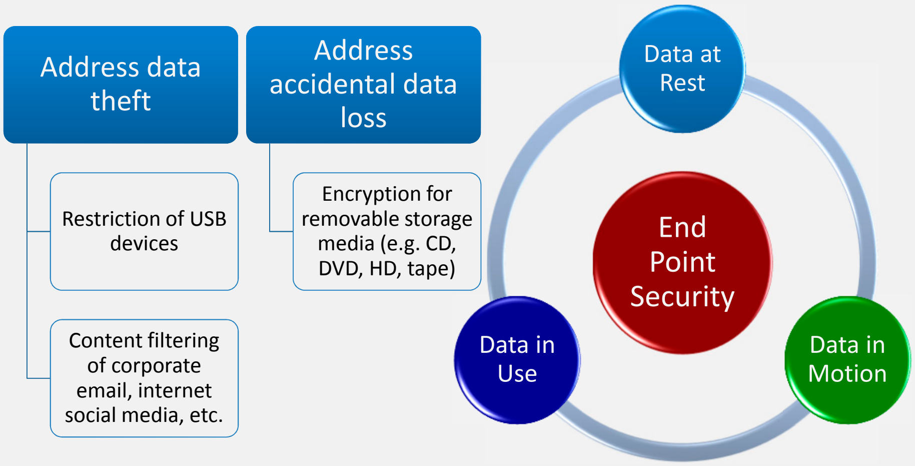
Austral Bank incident

Customers data have to be housed in Mozambique

Before 2003 *2013* *After 2003*

- A Notice was published in 2003 forcing all banks to have their customers data housed in Mozambique
  - 2013 ITRMG did not change that, but included a requirement on data processed by internal outsourcing partners…
    - it must be segregated from other data

Data Loss Prevention



Address data theft

- Restriction of USB devices
- Content filtering of corporate email, internet social media, etc.

Address accidental data loss

- Encryption for removable storage media (e.g. CD, DVD, HD, tape)

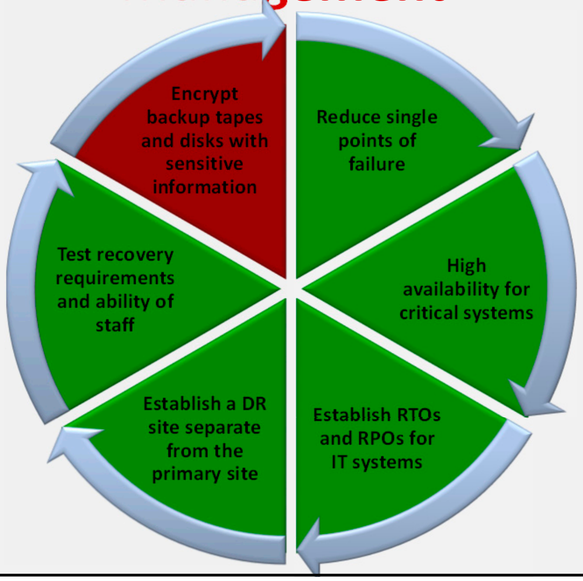
End Point Security

Data at Rest

Data in Motion

Data in Use

IT Continuity & Backup Management



Encrypt backup tapes and disks with sensitive information

Reduce single points of failure

High availability for critical systems

Establish RTOs and RPOs for IT systems

Establish a DR site separate from the primary site

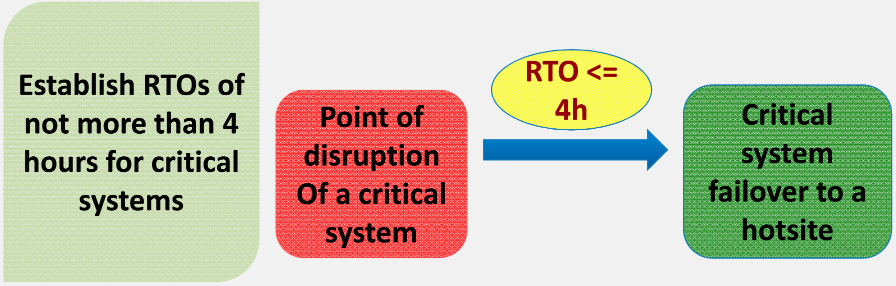
Test recovery requirements and ability of staff

Identification of Critical Systems

- Systems, the failure of which will…
  - cause significant **disruption to operations** (time critical operation)**,** or
  - materially **impact service to consumers** (essential services to customers)

*Banks should **establish a framework and process to identify critical systems**, and maintain a list of these*

RTOs for Critical Systems


Establish RTOs of not more than 4 hours for critical systems
Point of disruption Of a critical system
RTO <= 4h
Critical system failover to a hotsite

This is normally a challenge for most Mozambican banks

- *Real time synchronization between the original and duplicate sites does not come cheap!*

Shadow IT

- Identify important end user applications
- Include in recovery and support plans
- Apply similar reviews as for other bank applications and include them under IT approved solutions

Risk-based Approach to IT Supervision

– *IT Risk vs. Operational Risk*

– *Self-Assessment of IT Risks and Controls by the Banks*

– *ITRMG Mapping with COBIT Framework*

– *Examination Procedures*

IT Risk vs. Operational Risk

- BoM has created a practical way of separating the IT Risk from Operational Risk
  - IT risk has its rating schema:

BoM Risk Rating	COBIT Maturity Model
1: Minimal	5: Optimized
2: Moderate	3 and 4: Defined & Managed and Measurable
3: Significant	2: Repeatable but Intuitive
4: High	0 and 1: No-existent & Iniatial/*ad hoc*

  - IT examination results also inform the level of Operational Risk

Self-Assessment of IT Risks and Controls by the Banks

- Based on the approved ITRMG, an Excel self-assessment checklist was developed
  - The checklist has to be completed annually by the banks
  - Completed checklists and their supporting documents are submitted to BoM
- BoM reviews the banks' self-assessments in preparation of the on-site examinations
  - The review provides high level indication of the weaknesses in ITRM
  - Most significant weaknesses are considered for on-site examinations (plus other supervisory concerns)

ITRMG Mapping With COBIT Framework

- To keep examination procedures aligned with COBIT (*COBIT Assurance Guide*), the ITRMG were mapped with COBIT
  - The indexed guidelines sections were mapped to one or more of the 210 COBIT 4.1 control objectives
  - Some sections have no significant match with COBIT, thus their examination is based on professional judgement and other relevant materials
    - Industry-specific matters (like E-banking) could not be mapped
- The mapping also helps banks comply with the ITRMG and more effectively govern their IT

Examination Procedures

- Based on the examination scope and objectives, examination procedures might include:
  - The use of generalized audit software to survey the contents of data files (including system logs)
  - The use of specialized software to access the contents of OS, database and application parameter files (or detect deficiencies in system parameter settings)
  - Flow-charting techniques for documenting automated applications and business processes
  - The use of audit logs/reports available in operation/application systems

Examination Procedures

- Based on the examination scope and objectives, examination procedures might include:
  - Documentation review
  - Inquiry and observation
  - Walk-throughs
  - Re-performance of controls.

- **Comments and questions**
- **Thank you for attending!**