

An Interactive Panel on Business Operations Risk Assessments

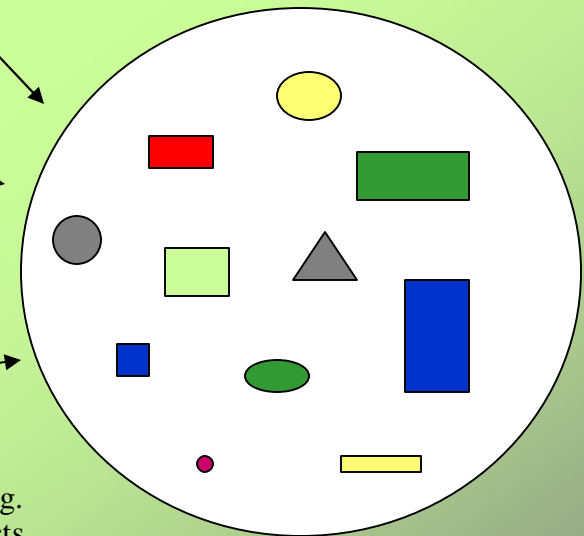
*Cal Braunstein, CEO
Robert Frances Group (RFG)*



The Categories of Risks

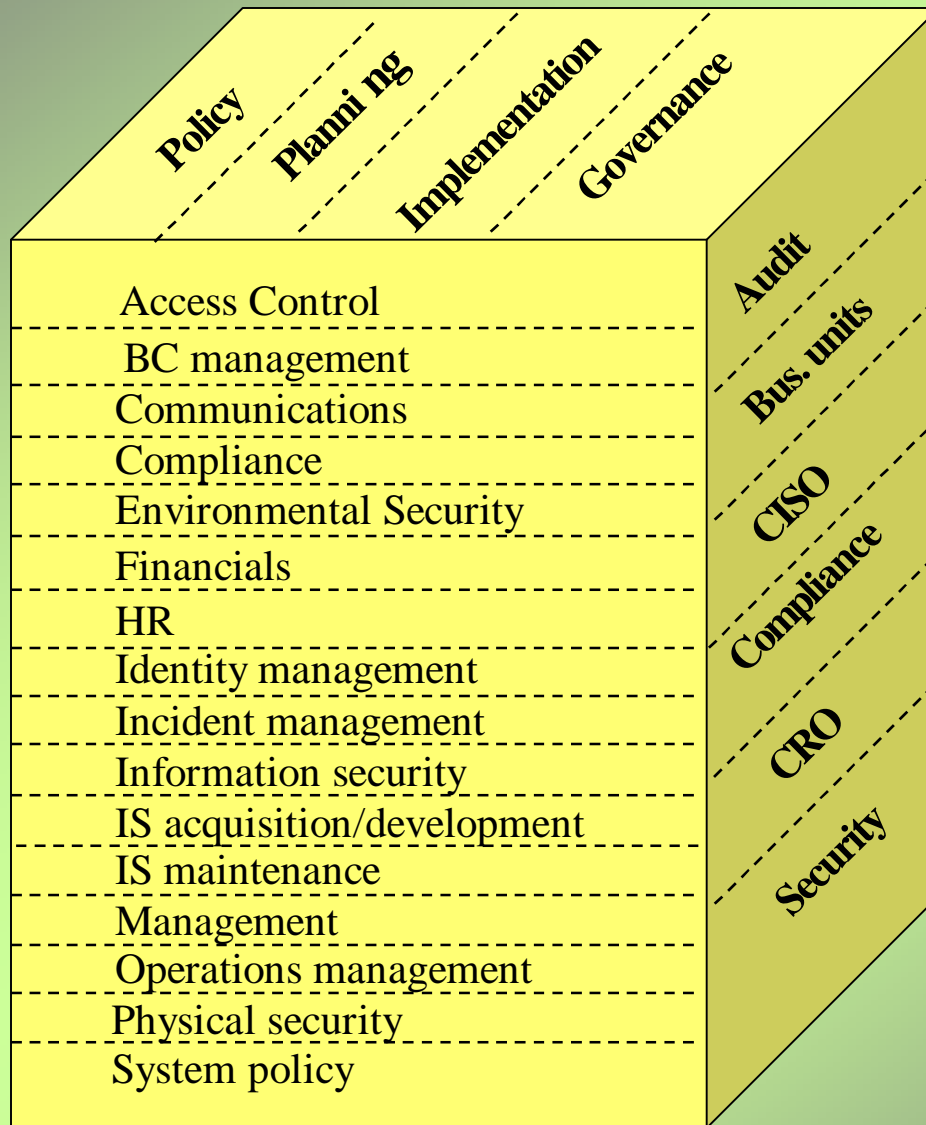
CATEGORY OF RISK DEFINITION

1. **Infrastructure** Relating to infrastructures such as transport systems for staff, power supply systems, suppliers, business relationships with partners, dependency on internet and e-mail.
 2. **Economic** Relating to economic factors such as interest rates, exchange rates, inflation.
 3. **Legal and Regulatory** Relating to the laws and regulations which if complied with should reduce hazards
 4. **Environmental** Relating to issues such as fuel consumption, pollution.
 5. **Political** Relating to possible political constraints such as change of government.
 6. **Market** Relating to issues such as competition and supply of goods.
 7. **"Act of God"** Relating to issues such as fire, flood, earthquake.
- External
8. **Budgetary** Relating to the availability of resources or the allocation of resources.
 9. **Fraud or theft** Relating to the unproductive loss of resources.
 10. **Insurable** Relating to potential areas of loss which can be insured against.
 11. **Capital Investment** Relating to the making of appropriate investment decisions.
 12. **Liability** Relating to the right to sue or to be sued in certain circumstances.
- Financial
13. **Policy** Relating to the appropriateness and quality of policy decisions.
 14. **Operational** Relating to the procedures employed to achieve particular objectives.
 15. **Information** Relating to the adequacy of information which is used for decision making.
 16. **Reputational** Relating to the public reputation of the organization and consequent effects.
 17. **Transferable** Relating to risks which may be transferred or to transfer of risks at inappropriate cost.
 18. **Technological** Relating to the use of technology to achieve objectives.
 19. **Project** Relating to project planning and management procedures.
 20. **Innovation** Relating to the exploitation of opportunities to make gains.
- Activity
21. **Personnel** Relating to the availability and retention of suitable staff.
 22. **Health and Safety** Relating to the well-being of people.
- Human Resources



Source: UK HM Treasury 2001

COSO/ISO business operational risk model



Risk Assessment Dashboard

Risk = threat* vulnerability* exposure	Threat	Vulnerability	Exposure
Confidentiality			
Integrity			
Availability			

Where

Threats are items such as people, nature, governments, competitors, etc.

Vulnerabilities are elements such as complexity, weak controls, inadequate governance, unencrypted data, etc.

Exposure relates to degree of criticality to the business, value of data, impacts of downtime

Risk Assessment Portfolio Dashboard

Risk Type	Potential Impact	Probability	Weighting Factor	Weighted Risk Exposure	Tolerance Level	Mitigation Option & Controls	Mitigation Required (Y/N)

Risk Weighting Factors

High or Unacceptable Risk Level	Medium or Acceptable Risk Level	Low or Acceptable Risk Level
1 event or a sum of events of adverse impact within 3 years of following nature:	1 event or a sum of events of adverse impact within 3 years of following nature:	1 event of adverse impact within 3 years of following nature:
Earnings charge of 1% or more, or about \$xx M pre-tax annually	Earnings charge of 0.25% to 0.99%, or about \$xx M pre-tax annually	Earnings charge of less than 25%, or about \$xx M pre-tax annually
Stock could drop by 7.5% or more relative to current price due to the news	Stock could drop by 2.5% to 7.5% relative to current price due to the news	Stock could drop by less than 2.5% relative to current price due to the news
Material regulatory or systematic risk	Questionable regulatory or systematic risk	Little or no regulatory or systematic risk

Panelists

- **Chris Kite**

VP of Enterprise Risk Management and
Workplace Resources, Cisco Systems

- **Kristy Spears**

Sr. VP line of business operational risk
executive, Bank of America

- **Mike Stiglianese**

Chief IT risk officer, Citigroup

Mapping Related Regulations to Simplify IT Risk Management – A Citigroup Approach



Basel II, Sarbanes Oxley and FFIEC all require assessments of operational risk, of which IT Risk is an integral component

Drivers of Citigroup IT Risk Management Solutions

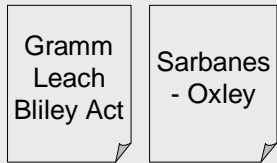
Emerging Risks

- * Coordinated terror attacks
- * Zombies and denial of service attacks
- * Extortion by criminal organizations

Headline-Grabbing Events*

- * "UPS Loses Citigroup Data on 3.9 Million Customers"
- * "Bank of America Consumer Data Tapes Lost"
- * "Time Warner employee data missing"

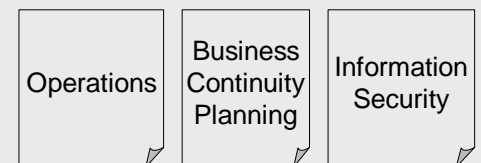
Regional Regulations



Global Regulations



Select FFIEC IT Handbooks



Sample Financial Institution Risk Management Solutions

Corrective Action Plan Tracking

Systems Inventory

IS Incident Management

Business Continuity Plans

3rd Party Access Registry

Risk Control Self Assessment tools

3rd Party IS Assessment

Company Policies and Directives

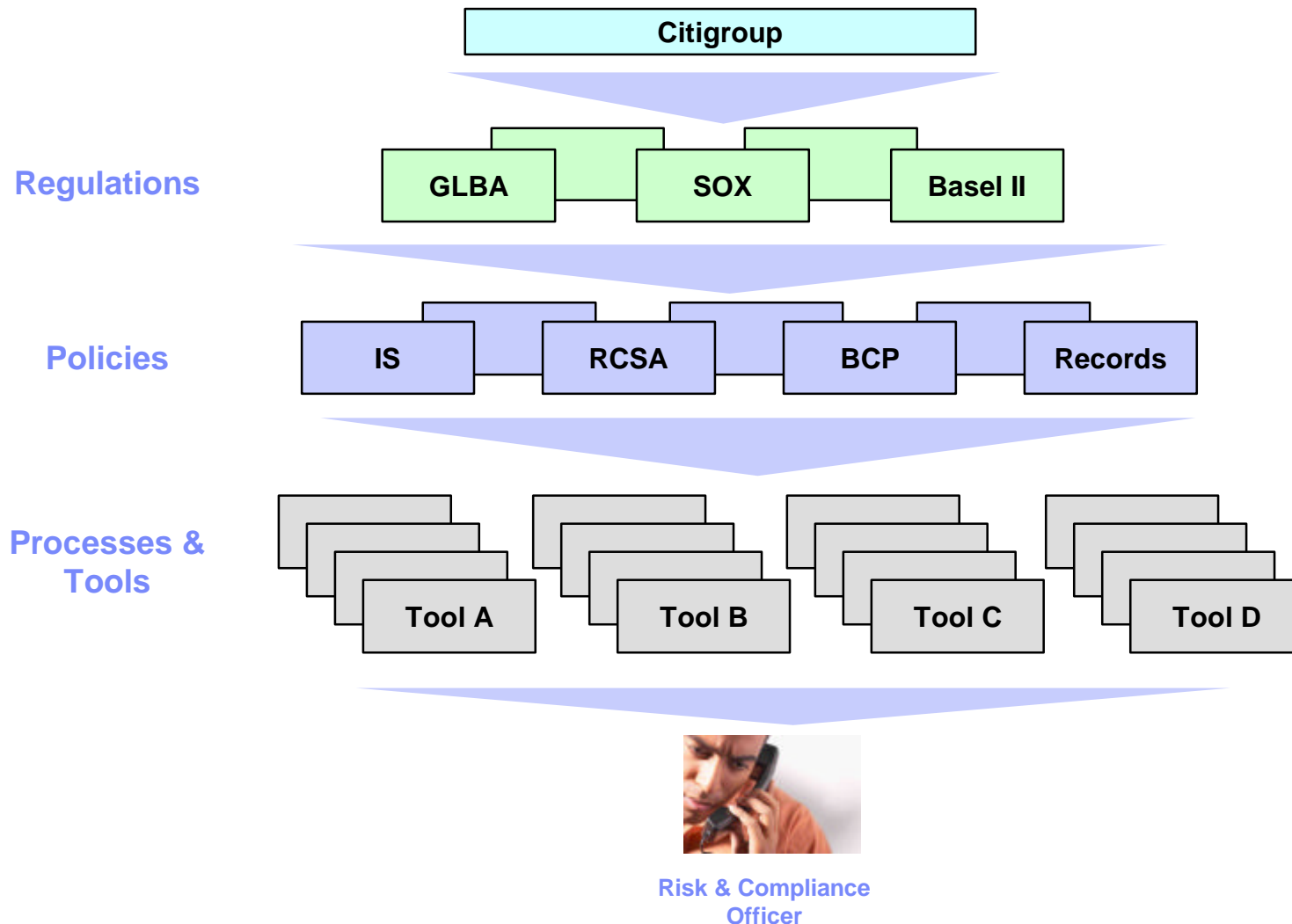
Information Security

Audit Policy

Operational Risk

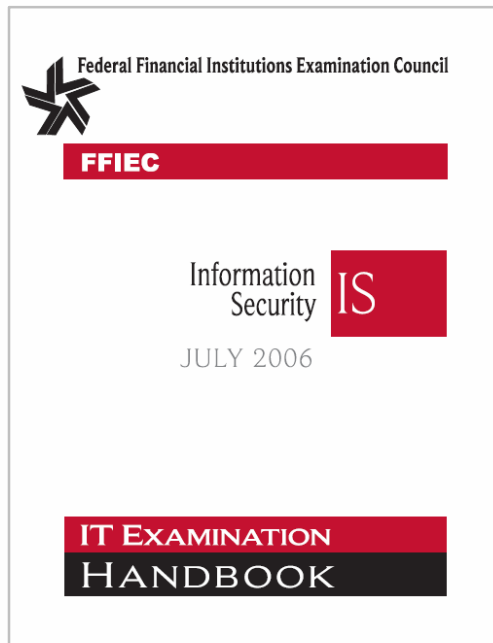
Self Assessment

As regulations increase, individual IS Risk and Compliance Officers become increasingly challenged to meet the mandated assessment requirements



A key requirement for the Integrated Risk Management Solution was to be able to accommodate changing regulatory requirements

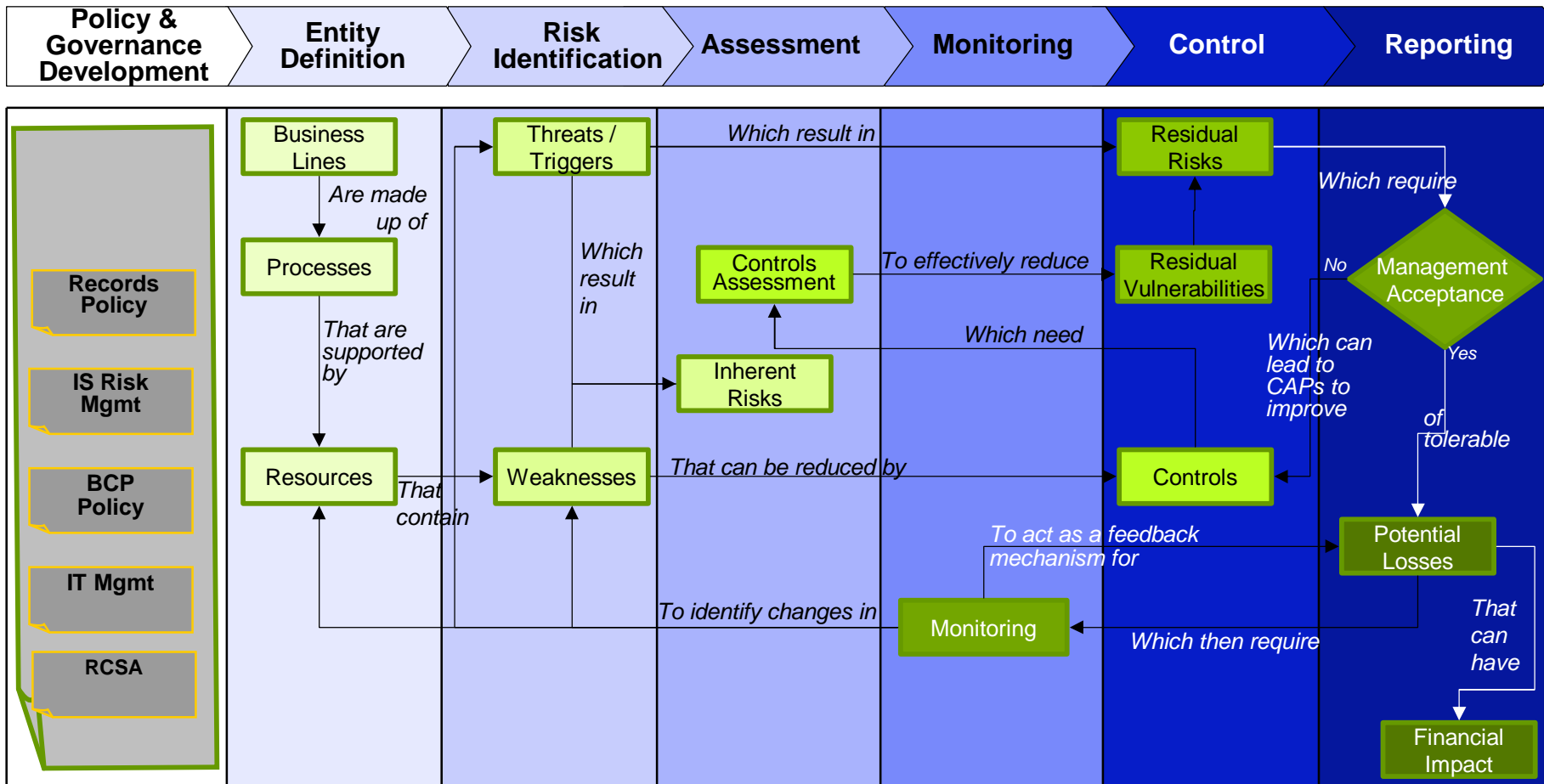
In July of 2006, the FFIEC issued a new Examination Handbook.....



Highlights of Significant Changes to the Handbook

- * Additional Focus on evaluating **Outsource Service Providers**
 - Evaluate outsourcing strategy to identify relevant data flows and information processing activities.
 - The institution's system architecture diagram and related documentation should identify service provider relationships, where and how data is passed between systems, and the relevant controls that are in place.
 - The evaluation of controls should also encompass the risks to information held and processed by service providers.
- * Distinguish **threats** from **vulnerabilities**
- * **Evaluate controls** that **prevent harm** as well as those that **detect harm** and correct damage

Regardless of the regulation, a common framework can be used for assessing and reporting IT, IS and operational risk



For the Information Security space, we are currently using the framework to address challenges related to information security risk assessments

Benefits of IRM Framework

- * Allows tracking of risk based on business hierarchy, process and resource views
- * Creates a library of risk events mapped to relevant regulations
- * Normalizes data entry through a standard set of controls and questionnaires
- * Ensures that management acceptance occurs for residual risk
- * Faster, easier reporting for line managers, senior management, regulators
- * Contains analytics to identify areas of risk
- * Provides ability to identify lessons learned based on repeated control failures
- * Provides tracking of non-compliance issues and action plans

 The framework was deployed first for Information Security and is now being extended to address RCSA

Q & A

