IT Risk and Control Framework

Mohammed Iqbal Hossain  
CISA, CGEIT  
Deputy Comptroller and Auditor General  
Office of the C&AG, Bangladesh,  
Board Member, ISACA Dhaka Chapter

Date: 25 February 2012
Session Objectives

- IT opportunities and risks
- Global concern/incidents
- Bangladesh perspective
- Best practices frameworks/standards
- ISACA COBIT framework
- Summary
Information is the key

- Information is the key resources
- We create information
- We use and store information
- We destroy information
- IT plays a key role in these activities
- Our duty is to protect these information asset

*http://www.dailytech.com/Worlds+Data+to+Reach+18+Zettabytes+by+2011/article11055.htm*
Technology creates opportunities

- Business online
- Education online
- Government online
- Provide E-health service
- Buy electronic contents (e-books, software, music etc)

*We can rich the whole world in a finger move*
Opportunity and Risk are two sides of the same coin
What are the IT Risks?

- Email password may be disclosed
- Facebook account may be used by someone else
- Credit card information may be disclosed
- Customer information may be stolen
- IT Service delivery to the customers may be poor
- IT systems may be obsolete
- IT projects may be late or fail
- IT systems do not provide any business benefit
- Risk of non-compliance with the regulator
- Own people may harm the systems

*IT risk is business risk*
Only one in eight IT projects can be considered truly successful (in terms of time, cost and quality)

The cost of project failure across the European Union was €142 billion in 2004

Source: http://www.bcs.org/content/ConWebDoc/19584
Incidents Reported by US Federal Agencies

http://www.gao.gov/products/GAO-12-137
E-crime is no longer driven by profit alone

Hackers are now state-sponsored and politically motivated

Simply defending systems against attack is not a sufficient strategy for today’s threat environment.

A complete approach needs to cover defence, detection, reaction and recovery

“The complexity of security challenges created by technology is only increasing”

http://www.kpmg.com/UK
Recent Cyber crime news

- Department of Homeland Security website hacked
- NASDAQ Site was track down with DDOS Attack
- Cyber attack crashes Irish government website
- Hackers Attack Second Brazilian Bank’s Website
- Ukraine Govt retreats after massive cyber-siege
- Zappos.com hacked; 24 million customers affected
- VeriSign Hit by Hackers in 2010
- Saudi hacker publishes Israeli credit card details
- Websites of 2 Palestinian news agencies brought down by cyber attack

Source: http://www.infowar.com/
ISACA Survey (2011)

- Increasing IT costs — 42%
- Insufficient IT skills — 33%
- Problems implementing new IT systems — 30%
- Problems with external IT service providers — 29%
- Serious operational IT incidents — 21%
- Return on investment not as expected — 19%
- IT security or privacy incidents — 18%

http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/ITGI-Global-Survey-Results.aspx
Bangladesh Scenario

Achievement

- Ranked 134 in UN E-Gov survey in e-gov development category
- Some quick win projects by Government
- Bangladesh is on the list of top 30 destinations for global IT outsourcing for 2010-11 (Gartner)

Challenges

- Ranked poor in language, infrastructure and data and intellectual property security (Gartner)
- Lack of sustainability of IT Systems
- Lack of ownership of IT systems
- Inadequate Human resources
- Poor IT management
- Increased cyber incidents
- No National BD-CERT
The impact of IT risks

- No organization is unaffected
- Businesses are disrupted
- Privacy is violated
- Organizations’ suffer direct financial loss
- Reputation is damaged
What is the solution

- No 100% solution
- We can not solve all the problems
- We can reduce to an acceptable level only
- Use best practices
Advantage of using Best Practices

- Better accountability and responsibility (ownership)
- No blame game
- Better management
- Better benefits from IT investments
- Better Compliance
- Better monitoring
- Compare with others
Some examples of best practice

- COBIT
- ITIL
- ISO 27001/2
- COSO ERM
- PRINCE2
- PMBOK
- Six Sigma
- TOGAF
About COBIT

- COBIT is a comprehensive IT governance and management framework.
- Accepted globally as a set of tools that ensures IT is working effectively and efficiently
- Addresses every aspect of IT
- Ensure clear ownership and responsibilities
- A common language for all
- Improves IT efficiency and effectiveness
- Better management of IT investments
- Ensure compliance
- Complementary copy is available (www.isaca.org/cobit)
COBIT Coverage

**PLAN & ORGANISE**
- Strategic IT Plan
- Manage IT Investment
- Manage IT Human Resources
- Manage IT Risks
- Manage Projects

**ACQUIRE & IMPLEMENT**
- Acquire & Maintain Application Software
- Acquire and Maintain Technology Infrastructure
- Manage Changes

**MONITOR & EVALUATE**
- Monitor and Evaluate IT Performance
- Monitor and Evaluate Internal Control
- Ensure Compliance
- Provide IT Governance

**DELIVERY & SUPPORT**
- Manage Third-party Services
- Ensure Continuous Service
- Ensure Systems Security
- Manage Incidents
- Manage data
- Manage Operations
## RACI Chart

### Activities

<table>
<thead>
<tr>
<th>Activities</th>
<th>Functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link business goals to IT goals.</td>
<td>C I A/R I C</td>
</tr>
<tr>
<td>Identify critical dependencies and current performance.</td>
<td>C C R A/R C C C C C C C</td>
</tr>
<tr>
<td>Build an IT strategic plan.</td>
<td>A C C R I C C C C I C</td>
</tr>
<tr>
<td>Build IT tactical plans.</td>
<td>C I A C C C C C R I</td>
</tr>
<tr>
<td><strong>ENSURE SYSTEM SECURITY (DS5)</strong></td>
<td></td>
</tr>
<tr>
<td>Define and Maintain IT Security Plan.</td>
<td>I C C A C C C C I I R</td>
</tr>
<tr>
<td>Conduct regular vulnerability assessments.</td>
<td>I A I C C C C R</td>
</tr>
</tbody>
</table>

A **RACI** chart identifies who is **Responsible**, **Accountable**, **Consulted** and/or **Informed**.
Define Goals and Metrics

Business Goal: Maintain Reputation

IT Goals: IT can resist from attack unauthorized access vulnerabilities and threats

Process Goal: Reduce unauthorized access

Activity Goal: Understand vulnerabilities and threats

Metrics:
- No of Incidents with public embarrassment
- No of incidents with business impact
- No of incidents because of unauthorized access
- Frequency of review
COBIT links Business goals to IT Process

- **Business Goals (17)**: Maintain IT Related Business Risk
  - Respond to governance requirements
  - Account for and protect all IT assets.
  - Protect the achievement of IT objectives.
  - Establish clarity of business impact
  - Ensure that critical and confidential information is authorized
  - Ensure that automated business transactions can be trusted.
  - Ensure that IT services and infrastructure can properly resist and recover from failures
  - Ensure minimum business impact in the event of an IT service disruption

- **IT Goals (28)**:

- **IT Processes (32)**:
  - Assess and manage IT risks (PO9)
  - Ensure systems security (DS5)
  - Manage the configuration (DS9)
  - Manage Facilities (DS12)
  - Monitor and evaluate internal control (ME2)
COBIT maps other frameworks

- ITIL
- ISO 27001/2
- ISO 20000
- PMBOK
- TOGAF
- CMMI
- COSO
COBIT maps with Basel II

COSO Components

Plan and Organize
Acquire and Implement
Deliver and Support
Monitor and Evaluate

COBIT Domains

Internal Environment
Objective Setting
Event Identification
Risk Assessment
Risk Response
Control Objectives
Control Activities
Information and Communication

Basel II Principles
- Board awareness and approval
- Independent internal audit
- Risk management framework
- Identification and assessment
- Monitoring operational risk
- Policies, processes and procedures
- Contingency and business continuity plans
- Banking supervision requirement for effective framework
- Banking supervision regular independent evaluation
- Sufficient public disclosure by banks

Source: IT Control Objectives for Basel II
Use Best practice such as COBIT to minimize IT Risks
Start with basic processes
Form a high level IT Strategy Committee headed by CEO/Head.
Formulate and implement IT Strategic Plan and IT policies.
Allocate resources (People, infrastructure,)
Assign roles and responsibilities, authority and accountability (Use RACI Chart)
Make IT a regular board agenda.
Regularly assess, review and monitor IT Risks.
Establish a national BD-CERT(by gov)
Thank You!

Questions?