Protecting Information Assets
- Week 4 -

Risk Evaluation

MIS5206 Week 4

- In the News
- Readings
  - 2009 Vacca Chapters 14, 35
  - 2012 Vacca Chapters 15, 35
  - HDFC BANK: SECURING ONLINE BANKING
  - ISACA RiskIT Framework pp. 47- 96
- Week 3 Material Highlights
- Risk Evaluation
- Test Taking Tip
- Quiz

In the News

http://fcw.com/articles/2014/09/12/trust-issues.aspx

It is no secret that the U.S. government is desperate to prevent another large-scale leak of classified information like the one carried out by Edward Snowden last year. And the role technology is playing in this pursuit could have long-term consequences for federal agencies' relationships with their employees.

Reading

- Vacca Chapter 15 – 35
- Case: HDFC BANK
- ISACA RiskIT Framework pp. 47 - 96

Week 3: Data Classification Process and Models

Information Category	Description	Examples
Unclassified Public	Information is not confidential and can be made public without any implications for Company. Loss of availability due to system downtime is an acceptable risk. Integrity is important but not vital.	• Product brochures widely distributed • Information widely available in the public domain, including publicly available Company web site areas • Sample downloads of Company software that is for sale • Financial reports required by regulatory authorities • Newsletters for external transmission
Proprietary	Information is restricted to management-approved internal access and protected from external access. Unauthorized access could influence Company's operational effectiveness, cause an important financial loss, provide a significant gain to a competitor, or cause a major drop in customer confidence. Information integrity is vital.	• Passwords and information on corporate security procedures • Know-how used to process client information • Standard Operating Procedures used in all parts of Company's business • All Company-developed software code, whether used internally or sold to clients
Client Confidential Data	Information received from clients in any form for processing in production by Company. The original copy of such information must not be changed in any way without written permission from the client. The highest possible levels of integrity, confidentiality, and restricted availability are vital.	• Client media • Electronic transmissions from clients • Product information generated for the client by Company production activities as specified by the client
Company Confidential Data	Information collected and used by Company in the conduct of its business to employ people, to log and fulfill client orders, and to manage all aspects of corporate finance. Access to this information is very restricted within the company. The highest possible levels of integrity, confidentiality, and restricted availability are vital.	• Salaries and other personnel data • Accounting data and internal financial reports • Confidential customer business data and confidential contracts • Non disclosure agreements with clients\vendors • Company business plans

Week 3: Data Classification Process and Models

Why is data classification important?

- Focuses attention on the identification and valuation of information assets
- Is the basis for access control policy and processes

Case: HDFC Banking

Let's discuss the case:

- What is the role of employee security awareness training in the overall security risk management strategy?
- To what extent should a company attempt to educate their customers about security concerns?
- What are some of the methods a company can use to raise security awareness?

Case: HDFC Banking

Case Study due 10/2:

- Via email
- Due by mid-night Tuesday 9/30

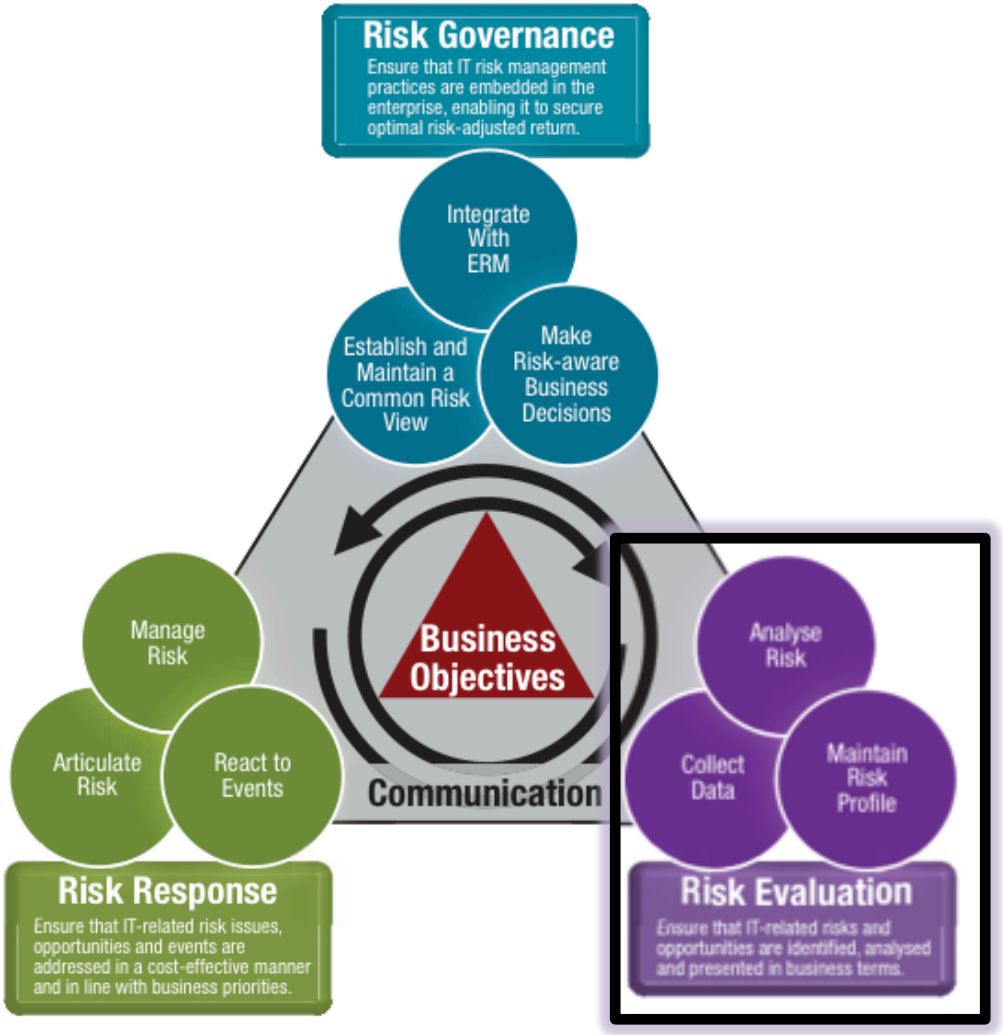
1. What if anything should HDFC do to make existing customers more secure?
2. How should HDFC deal with customers who, while signed-up, do not use online banking services?
3. At this point, should HDFC bank outsource secure data and transactions?

Risk Evaluation

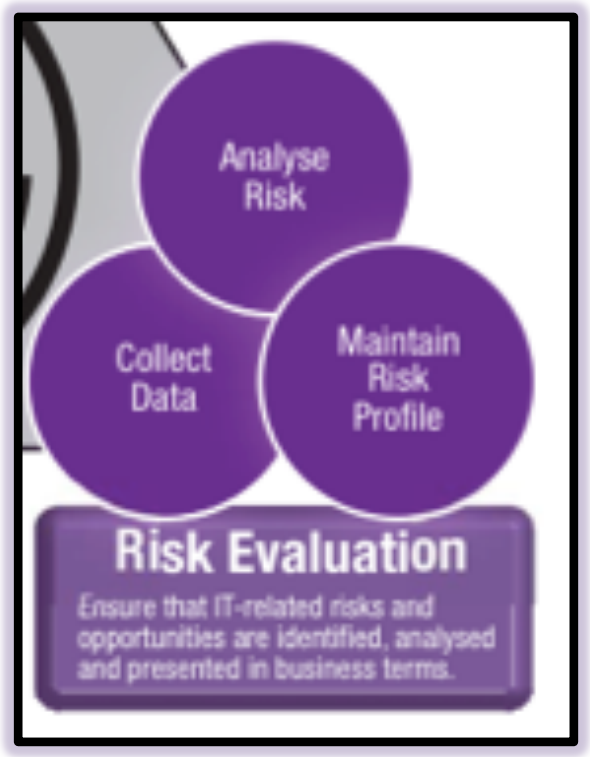
Risk evaluation is the process of identifying risk Risk Scenarios *and describing their potential* Business impact

The RiskIT Framework

The risk management process model groups key activities into a number of processes. These processes are grouped into three domains. The process model will appear familiar to users of COBIT and Val IT: substantial guidance is provided on the key activities within each process, responsibilities for the process, information flows between processes and performance management of the process.



Risk Evaluation - Key Components



Collect Data	Identify relevant data to enable effective IT-related risk identification, analysis and reporting
Analyze Risk	Develop useful information to support risk decisions that take into account the business impact of risk factors
Maintain Risk Profile	Maintain and up-to-date and complete inventory of known risks and attributes as understood in the context of IT controls and business processes

Collect Data

Goals and Metrics—RE1

Activity Goals	Process Goal	RE Goal
• Establish and maintain a model for data collection. • Collect data on the operating environment. • Collect data on risk events. • Identify risk factors.	• Identify relevant data to enable effective IT-related risk identification, analysis and reporting.	• Ensure that IT-related risks and opportunities are identified, analysed and presented in business terms.
Activity Metrics	**Process Metrics**	**RE Metric**
• Existence of a defined and documented risk-related data collection model • Number of sources used for data collection • Completeness of risk event data against established standards (e.g., affected assets, impact data, threat community, actions). This includes both discrete event data (e.g., control 'yes' or 'no') and continuous data (e.g., ongoing stream data on server response time). • Number of data items for which the contributing factors have been identified • Completeness of historical data across the top categories and domains of IT risk	• Number of loss events with key characteristics not captured in some form of repository • Degree to which collected data support reporting of trends and scenario analysis • The degree of visibility and recognition into the control state provided by data collection • The degree of visibility and recognition into the threat landscape provided by data collection	• The cumulative business impact from IT-related incidents and events not identified by risk evaluation processes

Collect Data

RACI Chart

Key Activities	Board	CEO	CRO	CIO	CFO	Enterprise Risk Committee	Business Management	Business Process Owner	Risk Control Functions	HR	Compliance and Audit
	Roles										
RE1.1 Establish and maintain a model for data collection.	I	I	A/R	C	C	C	C	C	C		C
RE1.2 Collect data on the operating environment.		I	A/R	C	I	I	C	I	I	I	C
RE1.3 Collect data on risk events.		I	A	R	C	I		C	C		I
RE1.4 Identify risk factors.			A	R	I	I	C	C	R	C	C

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Analyze Risk

Goals and Metrics

Activity Goals	Process Goal	Domain Goal
• Define IT risk analysis scope. • Estimate IT risk. • Identify risk response options. • Perform a peer review of IT risk analysis.	• Develop useful information to support risk decisions that take into account the business relevance of risk factors.	• Ensure that IT-related risks and opportunities are identified, analysed and presented in business terms.
Activity Metrics	**Process Metrics**	**Domain Metrics**
• Percentage of time analyses are substantiated by later experience or testing (accuracy) • Percentage of time that peer review finds no significant logical, calculation or incompleteness errors (defensibility) • Percentage of time that parallel assessments on the same scenarios performed by different analysts get the same results (consistency) • Percentage of time that analyses are performed by trained analysts (higher-level metric related to accuracy, defensibility and consistency) • A 'satisfaction index' derived over risk analysis reporting (e.g., the percentage of favourable satisfaction survey responses from business executives regarding the readability, usefulness and accuracy of risk analysis reports)	• Percentage of risks for which the probable frequency of occurrence and the probable magnitude of the business impact are measured within the scope • Percentage of critical assets, targets and resources reviewed for the effect of known operational controls • Percentage of risk analysis undergoing peer review before being sent to management • Ratio of cumulative actual losses to expected loss magnitude	• The cumulative business impact from IT-related incidents and events not identified by risk evaluation processes

Analyze Risk

MANAGEMENT GUIDELINES—RE2

RACI Chart **Roles**

Key Activities	Board	CEO	CRO	CIO	CFO	Enterprise Risk Committee	Business Management	Business Process Owner	Risk Control Functions	HR	Compliance and Audit
RE2.1 Define IT risk analysis scope.		I	R	C	I	C	A	R	C		C
RE2.2 Estimate IT risk.		I	R	C	C	I	A/R	R	R		C
RE2.3 Identify risk response options.			C	C	C	R	A	R	R		I
RE2.4 Perform a peer review of IT risk analysis.			A/R				I		I		I

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Maintain Risk Profile

Goals and Metrics

Activity Goals	Process Goal	RE Goal
• Map IT resources to business processes. • Determine business criticality of IT resources. • Understand IT capabilities. • Update IT risk scenario components. • Maintain the IT risk register and IT risk map. • Develop IT risk indicators.	• Maintain an up-to-date and complete inventory of known risks and attributes (e.g., expected frequency, potential impact, disposition), IT resources, capabilities and controls as understood in the context of business products, services and processes.	• Ensure that IT-related risks and opportunities are identified, analysed and presented in business terms.
Activity Metrics	**Process Metrics**	**RE Metric**
• Percentage of key business activities with a dependency linkage to supporting IT resources and IT infrastructure resources • Percentage of critical elements of the IT portfolio covered by risk triggers and thresholds • Frequency of updates to the IT risk scenario components • Number of significant internal or external change events not reviewed for impact on IT risk scenario components • Number of significant internal or external change events not reviewed for impact on the IT risk map • Number of realised events with business impact not detected by a trigger mechanism	• Number of approved risk analysis results not yet incorporated into the risk profile • Percentage of critical business services not covered by risk analysis • Completeness of attributes and values across IT risk scenario components • Completeness of key risk data attributes across the IT risk register	• The cumulative business impact from IT-related incidents and events not identified by risk evaluation processes

Maintain Risk Profile

RACI Chart

Key Activities	Board	CEO	CRO	CIO	CFO	Enterprise Risk Committee	Business Management	Business Process Owner	Risk Control Functions	HR	Compliance and Audit
	Roles										
RE3.1 Map IT resources to business processes.			I	R			C	A/R	C		I
RE3.2 Determine business criticality of IT resouces.		C		R		C	A	R			I
RE3.3 Understand IT capabilities.			C	A/R				C	C		I
RE3.4 Update IT risk scenario componenets.			C	R	I	C	C	A	R		C
RE3.5 Maintain the IT risk register and IT risk map.		I	A	R	I	I	I	R/C	C		I
RE3.6 Develop IT risk indicators.			A	C			C	C	R	C	C

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Test Taking Tip

- Eliminate any "probably wrong" answers first -

Focus on the "highest likelihood" answers for test taking efficiency

Here's why:

- Some of the answers use unfamiliar terms and stand out as unlikely and can therefore be discarded immediately
- Some answers are clearly wrong and you can recognize them based on your familiarity with the subject
- The correct answer may require a careful reading of the wording of the question and eliminating the unlikely answers early in the evaluation process helps you focus on key concepts for making the choice

Test Taking Tip

Example:

The promotion manager of Northeast Electronics has been made the owner of the department's printers and other resources. The manager can now designate who in the department can use the the large format printer. What term is used to describe this type of access control?

A. Mandatory
B. Role-Based
C. Discretionary
D. Distributed

Test Taking Tip

Example:

The promotion manager of Northeast Electronics has been made the owner of the department's printers and other resources. The manager can now designate who in the department can use the the large format printer. What term is used to describe this type of access control?

A. ~~Mandatory~~ Nothing seems mandatory about this scenario
B. Role-Based
C. Discretionary
D. Distributed

Test Taking Tip

Example:

The promotion manager of Northeast Electronics has been made the owner of the department's printers and other resources. The manager can now designate who in the department can use the the large format printer. What term is used to describe this type of access control?

A. ~~Mandatory~~
B. Role-Based Maybe ….
C. Discretionary
D. Distributed

Test Taking Tip

Example:

The promotion manager of Northeast Electronics has been made the owner of the department's printers and other resources. The manager can now designate who in the department can use the the large format printer. What term is used to describe this type of access control?

A. ~~Mandatory~~
B. ~~Role-Based~~ Nothing about roles other than manager in the question
C. Discretionary
D. Distributed

Test Taking Tip

Example:

The promotion manager of Northeast Electronics has been made the owner of the department's printers and other resources. The manager can now designate who in the department can use the the large format printer. What term is used to describe this type of access control?

A. ~~Mandatory~~
B. ~~Role-Based~~
C. Discretionary
D. Distributed

Test Taking Tip

Example:

The promotion manager of Northeast Electronics has been made the owner of the department's printers and other resources. The manager can now designate who in the department can use the the large format printer. What term is used to describe this type of access control?

A. ~~Mandatory~~
B. ~~Role-Based~~
C. Discretionary
D. Distributed

Answer: C

Quiz