Protecting Information Assets
- Week 4 -

Risk Evaluation
MIS5206 Week 4

• Readings
  – Vacca, Security Management Systems, Chapter 22
  – Vacca, Risk Management, Chapter 53
  – ISACA RiskIT Framework pp. 47-96

• Class
  – In the News
  – Week 3 Material Highlights
  – Risk Evaluation
  – Test Taking Tip
  – Quiz
In the News...
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
Week 3: Data classification process and models

What assets need protection?

What safeguards are available?

What techniques can identify incidents?

What techniques can contain impacts of incidents?

What techniques can restore capabilities?

IDENTIFY

PROTECT

DETECT

RESPOND

RECOVER
Risk evaluation is the process of identifying risk scenarios and describing their potential business impact.
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

<table>
<thead>
<tr>
<th>Activity Goals</th>
<th>Process Goal</th>
<th>RE Goal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establish and maintain a model for data collection.</td>
<td>Identify relevant data to enable effective IT-related risk identification, analysis and reporting.</td>
<td>Ensure that IT-related risks and opportunities are identified, analysed and presented in business terms.</td>
</tr>
<tr>
<td>Collect data on the operating environment.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Collect data on risk events.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identify risk factors.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Activity Metrics

<table>
<thead>
<tr>
<th>Process Metrics</th>
<th>RE Metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of loss events with key characteristics not captured in some form of repository</td>
<td>The cumulative business impact from IT-related incidents and events not identified by risk evaluation processes</td>
</tr>
<tr>
<td>Degree to which collected data support reporting of trends and scenario analysis</td>
<td></td>
</tr>
<tr>
<td>The degree of visibility and recognition into the control state provided by data collection</td>
<td></td>
</tr>
<tr>
<td>The degree of visibility and recognition into the threat landscape provided by data collection</td>
<td></td>
</tr>
</tbody>
</table>

---

**The Risk IT Framework**

-MIS 5206 Protecting Information Assets-
Collect Data

**RACI Chart**

<table>
<thead>
<tr>
<th>Key Activities</th>
<th>Board</th>
<th>CEO</th>
<th>CTO</th>
<th>CFO</th>
<th>Enterprise Risk Committee</th>
<th>Business Management</th>
<th>Business Process Owner</th>
<th>Risk Control Functions</th>
<th>HR</th>
<th>Compliance and Audit</th>
</tr>
</thead>
<tbody>
<tr>
<td>RE1.1 Establish and maintain a model for data collection.</td>
<td>I</td>
<td>I</td>
<td>A/R</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
</tr>
<tr>
<td>RE1.2 Collect data on the operating environment.</td>
<td>I</td>
<td>I</td>
<td>A/R</td>
<td>C</td>
<td>I</td>
<td>I</td>
<td>C</td>
<td>I</td>
<td>I</td>
<td>I</td>
</tr>
<tr>
<td>RE1.3 Collect data on risk events.</td>
<td>I</td>
<td>A</td>
<td>R</td>
<td>C</td>
<td>I</td>
<td>C</td>
<td>C</td>
<td>I</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RE1.4 Identify risk factors.</td>
<td>A</td>
<td>R</td>
<td>I</td>
<td>I</td>
<td>C</td>
<td>C</td>
<td>R</td>
<td>C</td>
<td>C</td>
<td></td>
</tr>
</tbody>
</table>

A **RACI** chart identifies who is **Responsible**, **Accountable**, **Consulted** and/or **Informed**.
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
## Analyze Risk

### Goals and Metrics

<table>
<thead>
<tr>
<th>Activity Goals</th>
<th>Process Goal</th>
<th>Domain Goal</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Define IT risk analysis scope.</td>
<td>• Develop useful information to support risk decisions that take into account the business relevance of risk factors.</td>
<td>• Ensure that IT-related risks and opportunities are identified, analysed and presented in business terms.</td>
</tr>
<tr>
<td>• Estimate IT risk.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Identify risk response options.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Perform a peer review of IT risk analysis.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Activity Metrics</th>
<th>Process Metrics</th>
<th>Domain Metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Percentage of time analyses are substantiated by later experience or testing (accuracy)</td>
<td>• Percentage of risks for which the probable frequency of occurrence and the probable magnitude of the business impact are measured within the scope</td>
<td>• The cumulative business impact from IT-related incidents and events not identified by risk evaluation processes</td>
</tr>
<tr>
<td>• Percentage of time that peer review finds no significant logical, calculation or incompleteness errors (defensibility)</td>
<td>• Percentage of critical assets, targets and resources reviewed for the effect of known operational controls</td>
<td></td>
</tr>
<tr>
<td>• Percentage of time that parallel assessments on the same scenarios performed by different analysts get the same results (consistency)</td>
<td>• Percentage of risk analysis undergoing peer review before being sent to management</td>
<td></td>
</tr>
<tr>
<td>• Percentage of time that analyses are performed by trained analysts (higher-level metric related to accuracy, defensibility and consistency)</td>
<td>• Ratio of cumulative actual losses to expected loss magnitude</td>
<td></td>
</tr>
<tr>
<td>• 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)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The Policy
The Agency head or designee has responsibility for ensuring agency information assets are appropriately categorized and the appropriate degree of protection is applied based on its valuation.

Background
To ensure that business information assets receive an appropriate level of protection, the value of the information must be assessed to determine the requirements for security protection. Business information assets are those that affect and are integral to the City's ability to provide business services with integrity, comply with laws and regulations, and meet public trust.

Scope
This policy applies to all information. Information is defined as anything spoken, overheard, written, stored electronically, copied, transmitted or held intellectually concerning the City of New York general business, information systems, employees, business partners, or customers.

Information Classification
All information at the City of New York and corresponding agencies will be classified at one of four levels: public, sensitive, private, or confidential.

- Public—This information might not need to be disclosed, but if it is, it shouldn't cause any damage.
- Sensitive—This information requires a greater level of protection to prevent loss of inappropriate disclosure.
- Private—This information is for agency use only, and its disclosure would damage the public trust placed in the agency.
- Confidential—This is the highest level of sensitivity, and disclosure could cause extreme damage to the agency's ability to perform its primary business function. Datasets containing information whose disclosure could lead directly to massive financial loss, danger to public safety, or lead to loss of life is classified as confidential.

Information Valuation and Categorization
1) Ensure that business information assets receive an appropriate level of protection. The value of the information must be assessed to determine the requirements for security protection.
2) All information assets must be valued and categorized.
3) Information assets must be evaluated, valued and categorized by the Data Steward on a regular basis.
4) To ensure that appropriate protection is provided, the value of information should be determined before transmission over any communications network.
The City of New York
CITYWIDE INFORMATION SECURITY POLICY

Data Classification Policy

The Policy
The Agency head or designee has responsibility for ensuring agency information assets are appropriately categorized and the appropriate degree of protection is applied based on its valuation.

Background
To ensure that business information assets receive an appropriate level of protection, the value of the information must be assessed to determine the requirements for security protection. Business information assets are those that affect and are integral to the City’s ability to provide business services with integrity, accuracy, and reliability.

Scope
This policy applies to all information written, stored electronically, or New York general business, its customers.

Information Classification
All information at the City of New York is at one of the four levels: public, sensitive, private, or confidential.
- Public—This information does not contain inappropriate disclosures.
- Sensitive—This information contains information that is sensitive, not public, or contains information with a high impact on the mission of the City
- Private—This information contains information that is private but does not contain the potential for danger to public safety, or lead to loss of life is classified as confidential.
- Confidential—This information contains information that is confidential and contains only information that is private and contains a high impact on the mission of the City.

Information Valuation and Categorization
1) Ensure that business information assets receive an appropriate level of protection. The value of the information must be assessed to determine the requirements for security protection.
2) All information assets must be valued and categorized.
3) Information assets must be evaluated, valued and categorized by the Data Steward on a regular basis.
4) To ensure that appropriate protection is provided, the value of information should be determined before transmission over any communications network.
Information Valuation and Categorization

1) Ensure that business information assets receive an appropriate level of protection. The value of the information must be assessed to determine the requirements for security protection.

2) All information assets must be valued and categorized.

3) Information assets must be evaluated, valued and categorized by the Data Steward on a regular basis.

4) To ensure that appropriate protection is provided, the value of information should be determined before transmission over any communications network.

Annualized loss expectancy (ALE) =

Single loss expectancy (SLE) \times \text{Annualized rate of occurrence (ARO)}

\text{Single loss expectancy (SLE)} = \text{Asset value} \times \text{Exposure factor}

\text{Annual rate of occurrence (ARO)} = \text{how many times is this expected to happen in one year?}
Information Valuation and Categorization

1) Ensure that business information assets receive an appropriate level of protection. The value of the information must be assessed to determine the requirements for security protection.

2) All information assets must be valued and categorized.

3) Information assets must be evaluated, valued and categorized by the Data Steward on a regular basis.

4) To ensure that appropriate protection is provided, the value of information should be determined before transmission over any communications network.

Information Classification

All information at the City of New York and corresponding agencies will be classified at one of four levels: public, sensitive, private, or confidential.

- **Public**—This information might not need to be disclosed, but if it is, it shouldn’t cause any damage.
- **Sensitive**—This information requires a greater level of protection to prevent loss of inappropriate disclosure.
- **Private**—This information is for agency use only, and its disclosure would damage the public trust placed in the agency.
- **Confidential**—This is the highest level of sensitivity, and disclosure could cause extreme damage to the agency’s ability to perform its primary business function. Datasets containing information whose disclosure could lead directly to massive financial loss, danger to public safety, or lead to loss of life is classified as confidential.
# FIPS 199: Risk event impact ratings

<table>
<thead>
<tr>
<th>Security Objective</th>
<th>POTENTIAL IMPACT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality</td>
<td></td>
</tr>
<tr>
<td>Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]</td>
<td>The unauthorized disclosure of information could be expected to have a <strong>limited</strong> adverse effect on organizational operations, organizational assets, or individuals. The unauthorized disclosure of information could be expected to have a <strong>serious</strong> adverse effect on organizational operations, organizational assets, or individuals. The unauthorized disclosure of information could be expected to have a <strong>severe or catastrophic</strong> adverse effect on organizational operations, organizational assets, or individuals.</td>
</tr>
<tr>
<td>Integrity</td>
<td></td>
</tr>
<tr>
<td>Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]</td>
<td>The unauthorized modification or destruction of information could be expected to have a <strong>limited</strong> adverse effect on organizational operations, organizational assets, or individuals. The unauthorized modification or destruction of information could be expected to have a <strong>serious</strong> adverse effect on organizational operations, organizational assets, or individuals. The unauthorized modification or destruction of information could be expected to have a <strong>severe or catastrophic</strong> adverse effect on organizational operations, organizational assets, or individuals.</td>
</tr>
<tr>
<td>Availability</td>
<td></td>
</tr>
<tr>
<td>Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]</td>
<td>The disruption of access to or use of information or an information system could be expected to have a <strong>limited</strong> adverse effect on organizational operations, organizational assets, or individuals. The disruption of access to or use of information or an information system could be expected to have a <strong>serious</strong> adverse effect on organizational operations, organizational assets, or individuals. The disruption of access to or use of information or an information system could be expected to have a <strong>severe or catastrophic</strong> adverse effect on organizational operations, organizational assets, or individuals.</td>
</tr>
</tbody>
</table>
FIPS 199: Composite IS risk event impact ratings

The generalized format for expressing the security category, SC, of an information system is:

\[
SC \text{ information system} = \{(\text{confidentiality, impact}), (\text{integrity, impact}), (\text{availability, impact})\},
\]

where the acceptable values for potential impact are LOW, MODERATE, or HIGH.

Example with multiple information types:

\[
SC \text{ contract information} = \{(\text{confidentiality, MODERATE}), (\text{integrity, MODERATE}), (\text{availability, LOW})\},
\]

and

\[
SC \text{ administrative information} = \{(\text{confidentiality, LOW}), (\text{integrity, LOW}), (\text{availability, LOW})\}.
\]

The resulting security category of the information system is expressed as:

\[
SC \text{ acquisition system} = \{(\text{confidentiality, MODERATE}), (\text{integrity, MODERATE}), (\text{availability, LOW})\},
\]
Analyzing risk

<table>
<thead>
<tr>
<th>Threat Likelihood</th>
<th>Low (10)</th>
<th>Moderate (50)</th>
<th>High (100)</th>
</tr>
</thead>
<tbody>
<tr>
<td>High (1.0)</td>
<td>10 x 1.0 = 10</td>
<td>50 x 1.0 = 50</td>
<td>100 x 1.0 = 100</td>
</tr>
<tr>
<td>Moderate (0.5)</td>
<td>10 x 0.5 = 5</td>
<td>50 x 0.5 = 25</td>
<td>100 x 0.5 = 50</td>
</tr>
<tr>
<td>Low (0.1)</td>
<td>10 x 0.1 = 1</td>
<td>50 x 0.1 = 5</td>
<td>100 x 0.1 = 10</td>
</tr>
</tbody>
</table>

Risk Scale: High (>50 to 100)  Moderate (>10 to 50)  Low (1 to 10)

Pironti’s recommendations...

- High – **Severe** material compliance, legal and/or financial consequences; significant material impact on critical business or operations processes; loss of customer trust and/or damage to brand reputation
- Medium – **Significant** material compliance, legal or financial consequences; substantial material impact on key business or operations processes; weakened customer trust and/or brand reputation
- Low – **Negligible**...

---

MIS 5206 Protecting Information Assets

### Material business impact - Financial

<table>
<thead>
<tr>
<th>Material Business Impact</th>
<th>Financial Loss Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catastrophic</td>
<td>US $100,000,000 and above</td>
</tr>
<tr>
<td>Major</td>
<td>US $5,000,000 to $99,999,999</td>
</tr>
<tr>
<td>Moderate</td>
<td>US $1,000,000 to $4,999,999</td>
</tr>
<tr>
<td>Minor</td>
<td>US $100,000 to $999,999</td>
</tr>
<tr>
<td>Negligible</td>
<td>Less than US $100,000</td>
</tr>
</tbody>
</table>

### Material business impact - Productivity

<table>
<thead>
<tr>
<th>Material Business Impact Category</th>
<th>Employee Productivity Percent Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catastrophic</td>
<td>85% and above</td>
</tr>
<tr>
<td>Major</td>
<td>40 - 84%</td>
</tr>
<tr>
<td>Moderate</td>
<td>20 - 39%</td>
</tr>
<tr>
<td>Minor</td>
<td>10 - 19%</td>
</tr>
<tr>
<td>Negligible</td>
<td>1 - 9%</td>
</tr>
</tbody>
</table>

### Material business impact - Availability

<table>
<thead>
<tr>
<th>Material Business Impact Category</th>
<th>Time of Unavailability (Partial or Full)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catastrophic</td>
<td>8 days and beyond</td>
</tr>
<tr>
<td>Major</td>
<td>73 hours - 7 days</td>
</tr>
<tr>
<td>Moderate</td>
<td>9 - 72 hours</td>
</tr>
<tr>
<td>Minor</td>
<td>2 - 8 hours</td>
</tr>
<tr>
<td>Negligible</td>
<td>Less than 2 hours</td>
</tr>
</tbody>
</table>

---

Analyze Risk

### MANAGEMENT GUIDELINES—RE2

**RACI Chart**

<table>
<thead>
<tr>
<th>Key Activities</th>
<th>Board</th>
<th>C3D</th>
<th>CRO</th>
<th>CIO</th>
<th>CFO</th>
<th>Enterprise Risk Committee</th>
<th>Business Management</th>
<th>Business Process Owner</th>
<th>Risk Control Functions</th>
<th>HR</th>
<th>Compliance and Audit</th>
</tr>
</thead>
<tbody>
<tr>
<td>RE2.1 Define IT risk analysis scope.</td>
<td>I</td>
<td>R</td>
<td>C</td>
<td>I</td>
<td>C</td>
<td>A</td>
<td>R</td>
<td>C</td>
<td>C</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RE2.2 Estimate IT risk.</td>
<td>I</td>
<td>R</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>A/R</td>
<td>R</td>
<td>R</td>
<td>C</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RE2.3 Identify risk response options.</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>R</td>
<td>A</td>
<td>R</td>
<td>R</td>
<td>I</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RE2.4 Perform a peer review of IT risk analysis.</td>
<td>A/R</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

A **RACI** chart identifies who is **Responsible**, **Accountable**, **Consulted and/or Informed**.
Data Classification Policy

The Policy
The Agency head or designee has responsibility for ensuring agency information assets are appropriately categorized and the appropriate degree of protection is applied based on its valuation.

Background
To ensure that business information assets receive an appropriate level of protection, the value of the information must be assessed to determine the requirements for security protection. Business information assets are those that affect and are integral to the City’s ability to provide business services with integrity, comply with laws and regulations, and meet public trust.

Scope
This policy applies to all information. Information is defined as anything spoken, overheard, written, stored electronically, copied, transmitted or held intellectually concerning the City of New York general business, information systems, employees, business partners, or customers.

Information Classification
All information at the City of New York and corresponding agency, four levels; public, sensitive, private, or confidential.
- Public—This information might not need to be disclosed, but damage.
- Sensitive—This information requires a greater level of protection and appropriate disclosure.
- Private—This information is for agency use only, and its disclosure would place the agency in public trust placed in the agency.
- Confidential—This is the highest level of sensitivity, and damage to the agency’s ability to perform its primary business, containing information whose disclosure could lead directly to danger to public safety, or lead to loss of life is classified as confidential.

Information Valuation and Categorization
1) Ensure that business information assets receive an appropriate valuation. The value of the information must be assessed to determine appropriate security protection.
2) All information assets must be valued and categorized.
3) Information assets must be evaluated, valued and categorized on a regular basis.
4) To ensure that proper protection is provided, the value must be determined before transmission over any communication channel.

Data Steward
5) The Data Steward is normally someone who is responsible for or dependent on the business process associated with the information asset, and who is knowledgeable about how the information is acquired, transmitted, stored, deleted, and otherwise processed.
6) The Data Steward is responsible for determining the appropriate value and categorization of the information generated by the owner or the Agency.
7) The Data Steward must communicate the information value and categorization when the information is released or provided to another entity.
8) The Data Steward is responsible for controlling access to his/her information and must be consulted when other entities wish to extend access authority.
## Maintain Risk Profile

### Goals and Metrics

<table>
<thead>
<tr>
<th>Activity Goals</th>
<th>Process Goal</th>
<th>RE Goal</th>
</tr>
</thead>
</table>
| - 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. |

<table>
<thead>
<tr>
<th>Activity Metrics</th>
<th>Process Metrics</th>
<th>RE Metric</th>
</tr>
</thead>
</table>
| - 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 |
The City of New York
CITYWIDE INFORMATION SECURITY POLICY

Data Classification Policy

The Policy
The Agency head or designee has responsibility for ensuring agency information assets are appropriately categorized and the appropriate degree of protection is applied based on its valuation.

Background
To ensure that business information assets receive an appropriate level of protection, the value of the information must be assessed to determine the requirements for security protection. Business information assets are those that affect and are integral to the City’s ability to provide business services with integrity, comply with laws and regulations, and meet public trust.

Scope
This policy applies to all information. Information is defined as anything spoken, overheard, written, stored electronically, copied, transmitted or held intellectually concerning the City of New York general business, information systems, employees, business partners, or customers.

Information Classification
All information at the City of New York and corresponding agencies will be classified at one of four levels: public, sensitive, private, or confidential.
- Public—This information might not need to be disclosed, but if it is, it shouldn’t cause any damage.
- Sensitive—This information requires a greater level of protection to prevent loss of inappropriate disclosure.
- Private—This information is for agency use only, and its disclosure would damage the public trust placed in the agency.
- Confidential—This is the highest level of sensitivity, and disclosure could cause extreme damage to the agency’s ability to perform its primary business function. Datasets containing information whose disclosure could lead directly to massive financial loss, danger to public safety, or lead to loss of life is classified as confidential.

Information Valuation and Categorization
1) Ensure that business information assets receive an appropriate level of protection. The value of the information must be assessed to determine the requirements for security protection.
2) All information assets must be valued and categorized.
3) Information assets must be evaluated, valued and categorized by the Data Steward on a regular basis.
4) To ensure that appropriate protection is provided, the value of information should be determined before transmission over any communications network.

Updated September 9, 2014 Version 1.5
PUBLIC Use pursuant to City of New York guidelines
Page 1 of 3
**Maintain Risk Profile**

### Key Activities

<table>
<thead>
<tr>
<th>Activity</th>
<th>Board</th>
<th>CED</th>
<th>CTO</th>
<th>CFO</th>
<th>Enterprise Risk Committee</th>
<th>Business Management</th>
<th>Business Process Owner</th>
<th>Risk Control Functions</th>
<th>HR</th>
<th>Compliance and Audit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Map IT resources to business processes</td>
<td>I</td>
<td>R</td>
<td>C</td>
<td>A/R</td>
<td>C</td>
<td>A/R</td>
<td>C</td>
<td>I</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Determine business criticality of IT resources</td>
<td>C</td>
<td>R</td>
<td>C</td>
<td>A/R</td>
<td>C</td>
<td>A/R</td>
<td>C</td>
<td>I</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Understand IT capabilities</td>
<td>C</td>
<td>R</td>
<td>C</td>
<td>A/R</td>
<td>C</td>
<td>A/R</td>
<td>C</td>
<td>I</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Update IT risk scenario components</td>
<td>C</td>
<td>R</td>
<td>I</td>
<td>C</td>
<td>A/R</td>
<td>C</td>
<td>A/R</td>
<td>C</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maintain the IT risk register and IT risk map</td>
<td>I</td>
<td>A/R</td>
<td>R</td>
<td>I</td>
<td>I</td>
<td>R/C</td>
<td>C</td>
<td>I</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Develop IT risk indicators</td>
<td>A</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>R</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

---

### Data Steward

5) The Data Steward is normally someone who is responsible for or dependent on the business process associated with the information asset, and who is knowledgeable about how the information is acquired, transmitted, stored, deleted, and otherwise processed.

6) The Data Steward is responsible for determining the appropriate value and categorization of the information generated by the owner or the Agency.

7) The Data Steward must communicate the information value and categorization when the information is released or provided to another entity.

8) The Data Steward is responsible for controlling access to his/her information and must be consulted when other entities wish to extend access authority.
Case: HDFC Banking

Let’s discuss the case:

Article is a bit dated, since it was written online adoption and use has increased exponentially.

Is online banking in India still in awareness creation mode?

Generationally...?

Age is a big issue – older folks want face to face “guarantee” for their transactions

Geographically...?

City dwellers versus country dwellers is a big thing!

Country dwellers...

• Anything that is tangible, that customers can touch they can trust
• To many in the country - online is not tangible, if they cannot physically see/touch the bank teller then there is a believe it cannot be trusted
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

Let’s discuss the case:

• What if anything should HDFC do to make existing customers more secure?

• How should HDFC deal with customers who, while signed-up, do not use online banking services?

• At this point, should HDFC bank outsource secure data and transactions?
HDFC Case Analysis Write Up

1. What are the security challenges in online banking?

2. What are the issues of security that are unique to online banking in India?

3. What are the challenges faced by Salvi?

4. How should Salvi address the issues before him?
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 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
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 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

Nothing seems mandatory about this scenario.
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 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
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 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
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 large format printer. What term is used to describe this type of access control?

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

Distributed is not relevant to the information in the question
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 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