The examination of ICAP is a grueling test of students’ abilities to master a range of subjects to ensure that those who qualify are consummate professionals.

The subject of Information Technology Management Audit & Control is deemed difficult by many due to the fact that most of the trainee students do not have a hands-on experience and understanding of the subject. The fact that there is no indicative-grid for ITMAC adds fuel to students’ agony and hence the paper pattern cannot be determined or guessed easily.

The published version of ITMAC COMPENDIUM is a combination of my class-notes, slides and past papers along with their solutions, hence providing a holistic solution for preparation of ITMAC exams for CA Final students. The online version consists of the slides/presentation used for teaching in class.

I hope ITMAC COMPENDIUM will help you in passing the subject. Feedback will be highly appreciated and can be sent to my email address given at the end of the preface.

Kindly remember me in your prayers.

Bilal Mahmood Sulehri - M.Phil (Contd.), MBA, ACPA, ACFA CICA, Oracle Certified Expert
bilal@sulehri.com

January 31, 2015
# ITMAC PAST PAPER ANALYSIS

## Topic: IT Strategy

<table>
<thead>
<tr>
<th>W-15</th>
<th>S-15</th>
<th>W-14</th>
<th>S-14</th>
<th>W-13</th>
<th>S-13</th>
<th>W-12</th>
<th>S-12</th>
<th>W-11</th>
<th>S-11</th>
<th>W-10</th>
<th>Total</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>14</td>
<td>10</td>
<td>9</td>
<td>15</td>
<td>-</td>
<td>-</td>
<td>10</td>
<td>11</td>
<td>18</td>
<td>9</td>
<td>-</td>
<td>96</td>
<td>8.7%</td>
</tr>
</tbody>
</table>

## Topic: E-Business

<table>
<thead>
<tr>
<th>W-15</th>
<th>S-15</th>
<th>W-14</th>
<th>S-14</th>
<th>W-13</th>
<th>S-13</th>
<th>W-12</th>
<th>S-12</th>
<th>W-11</th>
<th>S-11</th>
<th>W-10</th>
<th>Total</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>14</td>
<td>15</td>
<td>10</td>
<td>7</td>
<td>11</td>
<td>14</td>
<td>8</td>
<td>12</td>
<td>12</td>
<td>-</td>
<td>-</td>
<td>103</td>
<td>9.4%</td>
</tr>
</tbody>
</table>

## Topic: Management, P&D of IT

<table>
<thead>
<tr>
<th>W-15</th>
<th>S-15</th>
<th>W-14</th>
<th>S-14</th>
<th>W-13</th>
<th>S-13</th>
<th>W-12</th>
<th>S-12</th>
<th>W-11</th>
<th>S-11</th>
<th>W-10</th>
<th>Total</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>10</td>
<td>31</td>
<td>10</td>
<td>21</td>
<td>35</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>151</td>
<td>13.7%</td>
</tr>
</tbody>
</table>

## Topic: SCM

<table>
<thead>
<tr>
<th>W-15</th>
<th>S-15</th>
<th>W-14</th>
<th>S-14</th>
<th>W-13</th>
<th>S-13</th>
<th>W-12</th>
<th>S-12</th>
<th>W-11</th>
<th>S-11</th>
<th>W-10</th>
<th>Total</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.0</td>
<td></td>
</tr>
</tbody>
</table>

## Topic: ERP

<table>
<thead>
<tr>
<th>W-15</th>
<th>S-15</th>
<th>W-14</th>
<th>S-14</th>
<th>W-13</th>
<th>S-13</th>
<th>W-12</th>
<th>S-12</th>
<th>W-11</th>
<th>S-11</th>
<th>W-10</th>
<th>Total</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>5</td>
<td>6</td>
<td>13</td>
<td>-</td>
<td>11</td>
<td>43</td>
<td>3.9%</td>
</tr>
</tbody>
</table>

## Topic: CRM

<table>
<thead>
<tr>
<th>W-15</th>
<th>S-15</th>
<th>W-14</th>
<th>S-14</th>
<th>W-13</th>
<th>S-13</th>
<th>W-12</th>
<th>S-12</th>
<th>W-11</th>
<th>S-11</th>
<th>W-10</th>
<th>Total</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.0</td>
<td></td>
</tr>
</tbody>
</table>

## Topic: SFA

<table>
<thead>
<tr>
<th>W-15</th>
<th>S-15</th>
<th>W-14</th>
<th>S-14</th>
<th>W-13</th>
<th>S-13</th>
<th>W-12</th>
<th>S-12</th>
<th>W-11</th>
<th>S-11</th>
<th>W-10</th>
<th>Total</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>13</td>
<td>1.2%</td>
</tr>
</tbody>
</table>

## Topic: IS Audit, Processes & Controls

<table>
<thead>
<tr>
<th>W-15</th>
<th>S-15</th>
<th>W-14</th>
<th>S-14</th>
<th>W-13</th>
<th>S-13</th>
<th>W-12</th>
<th>S-12</th>
<th>W-11</th>
<th>S-11</th>
<th>W-10</th>
<th>Total</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>42</td>
<td>35</td>
<td>-</td>
<td>16</td>
<td>13</td>
<td>10</td>
<td>141</td>
<td>12.8%</td>
</tr>
</tbody>
</table>

## Topic: SDLC

<table>
<thead>
<tr>
<th>W-15</th>
<th>S-15</th>
<th>W-14</th>
<th>S-14</th>
<th>W-13</th>
<th>S-13</th>
<th>W-12</th>
<th>S-12</th>
<th>W-11</th>
<th>S-11</th>
<th>W-10</th>
<th>Total</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>8</td>
<td>20</td>
<td>9</td>
<td>10</td>
<td>12</td>
<td>10</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>14</td>
<td>92</td>
<td>8.4%</td>
</tr>
</tbody>
</table>

## Topic: Auditing Infrastructure & Operations

<table>
<thead>
<tr>
<th>W-15</th>
<th>S-15</th>
<th>W-14</th>
<th>S-14</th>
<th>W-13</th>
<th>S-13</th>
<th>W-12</th>
<th>S-12</th>
<th>W-11</th>
<th>S-11</th>
<th>W-10</th>
<th>Total</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>27</td>
<td>10</td>
<td>-</td>
<td>-</td>
<td>17</td>
<td>-</td>
<td>15</td>
<td>-</td>
<td>10</td>
<td>79</td>
<td>7.2%</td>
<td></td>
</tr>
</tbody>
</table>

## Topic: Protection of Information Assets

<table>
<thead>
<tr>
<th>W-15</th>
<th>S-15</th>
<th>W-14</th>
<th>S-14</th>
<th>W-13</th>
<th>S-13</th>
<th>W-12</th>
<th>S-12</th>
<th>W-11</th>
<th>S-11</th>
<th>W-10</th>
<th>Total</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>19</td>
<td>16</td>
<td>11</td>
<td>27</td>
<td>12</td>
<td>25</td>
<td>10</td>
<td>-</td>
<td>9</td>
<td>15</td>
<td>145</td>
<td>13.2%</td>
<td></td>
</tr>
</tbody>
</table>

## Topic: Disaster Recovery & BCP

<table>
<thead>
<tr>
<th>W-15</th>
<th>S-15</th>
<th>W-14</th>
<th>S-14</th>
<th>W-13</th>
<th>S-13</th>
<th>W-12</th>
<th>S-12</th>
<th>W-11</th>
<th>S-11</th>
<th>W-10</th>
<th>Total</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>12</td>
<td>13</td>
<td>-</td>
<td>16</td>
<td>10</td>
<td>15</td>
<td>11</td>
<td>-</td>
<td>10</td>
<td>7</td>
<td>125</td>
<td>11.4%</td>
</tr>
</tbody>
</table>

## Topic: Ron Weber

<table>
<thead>
<tr>
<th>W-15</th>
<th>S-15</th>
<th>W-14</th>
<th>S-14</th>
<th>W-13</th>
<th>S-13</th>
<th>W-12</th>
<th>S-12</th>
<th>W-11</th>
<th>S-11</th>
<th>W-10</th>
<th>Total</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>2</td>
<td>8</td>
<td>-</td>
<td>-</td>
<td>7</td>
<td>12</td>
<td>21</td>
<td>7</td>
<td>25</td>
<td>18</td>
<td>103</td>
<td>9.4%</td>
</tr>
</tbody>
</table>

## Topic: Improve

<table>
<thead>
<tr>
<th>W-15</th>
<th>S-15</th>
<th>W-14</th>
<th>S-14</th>
<th>W-13</th>
<th>S-13</th>
<th>W-12</th>
<th>S-12</th>
<th>W-11</th>
<th>S-11</th>
<th>W-10</th>
<th>Total</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>10</td>
<td>1.7%</td>
</tr>
</tbody>
</table>

## Topic: COBIT

<table>
<thead>
<tr>
<th>W-15</th>
<th>S-15</th>
<th>W-14</th>
<th>S-14</th>
<th>W-13</th>
<th>S-13</th>
<th>W-12</th>
<th>S-12</th>
<th>W-11</th>
<th>S-11</th>
<th>W-10</th>
<th>Total</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>-</td>
<td>8</td>
<td>-</td>
<td>-</td>
<td>7</td>
<td>12</td>
<td>21</td>
<td>7</td>
<td>68</td>
<td>21</td>
<td>6.2%</td>
<td></td>
</tr>
</tbody>
</table>

## Topic: TOTAL

<table>
<thead>
<tr>
<th>W-15</th>
<th>S-15</th>
<th>W-14</th>
<th>S-14</th>
<th>W-13</th>
<th>S-13</th>
<th>W-12</th>
<th>S-12</th>
<th>W-11</th>
<th>S-11</th>
<th>W-10</th>
<th>Total</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>1,100</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note:**
- This analysis is only for identifying trends in ICAP exams; no decision (of selective study) should be taken based on this analysis.
- All topics are equally important as there is no indicative grid in ITMAC.
- To err is human. This analysis has been compiled with due care but it may contain human error.
- In case of any error or omission, send an e-mail to bilal@sulehri.com with reference to the specific cell. Your feedback will be highly appreciated.
IT STRATEGY & MANAGEMENT

IT STRATEGY

- Strategy is a topic of BM and you should focus on understanding it there.

- The word “strategy” comes from Greek word Strategos which means “generalship”

- Strategy is a pattern of activities that seek to achieve the objective of the organization and adapt its scope, resources and operations on environmental changes in the long term
  - Strategy is a pattern of activities
  - Strategy is concerned with achieving objectives

by: Bilal Mahmood Sulehri
LEVELS OF STRATEGY

- Corporate strategy: It is concerned with what types of business the organization is in. It denotes the most general level of strategy in an organization.

- Business strategy: It is concerned with how an organization approaches a particular product or market.

- Functional or operational strategy: How the different functions of the business support the corporate and business strategies.

STRATEGIC PLAN

- Strategic planning is a disciplined effort to produce fundamental decisions and actions that shape and guide what an organization is, what it does, and why it does it, with a focus on the future.

- The strategic plan provides:
  - A framework for decisions or for securing support
  - Provide a basis for more detailed planning
  - Explain the business to others in to inform, motivate and involve
  - Assist performance monitoring
  - Stimulate change and become building block for next plan
STRATEGIC PLANNING PROCESS

Planning Stage
- Strategic Analysis
- Strategic Choice
- Strategic Implementation

Component of Plan
- Mission
- Goals
- Strategies
- Policies
- Decisions
- Actions

Key Question
- What business are we in?
- Where are we going?
- Which routes have we selected?
- What sort of framework is needed?
- What choices do we have?
- How shall we do it?

by: Bilal Mahmood Sulehri

---

STRATEGIC PLANNING

- Benefits of strategic planning
  - Clearly define purpose of organization
  - Communication of goals and objectives etc.

- Guidelines for preparing the strategic plan
  - Use a cross-functional team
  - Ensure the plan is realistic
  - Specify roles and responsibilities clearly
  - Should be reflected in job descriptions and personnel performance reviews
  - Follow-ups to the plan
  - One person should have the ultimate responsibility of implementing the plan
  - CEO's support
  - Feedback
  - Checkers – e.g. quarterly verification

by: Bilal Mahmood Sulehri
**IT STRATEGIC PLAN**

- **Business/corporate strategy**
- **Divisional strategy**
- **IS strategy**
  - **IT strategy**
  - **Communication strategy**
    - **Hardware**
    - **Software**
    - **Data**
    - **Voice**
- **Market strategy**
- **Production strategy**

by: Bilal Mahmood Sulehri

---

**STRATEGIC PLANNING**

- **Purpose/end result of an IS strategic plan:**
  - Effective management of expensive & critical assets of organization
  - Linking the IS direction to business direction
  - Planning the flow of information and processes
  - Efficiently and effectively allocation IS resources
  - Reducing the time and expense of the IS life cycle

- **Components of strategic planning (Gap analysis):**
  - Identification of where we are today
  - Identification of where we want to be in future
  - Identification of the gap
  - Identification of how to get IS to where we want to be in future

by: Bilal Mahmood Sulehri
**STRATEGIC PLANNING**

- Elements of an IS strategic plan:
  - Executive summary
  - Goals
  - Assumptions
  - Scenario
  - Application areas
  - Operations
  - Maintenance
  - Organizational structure
  - Impact of the plan

by: Bilal Mahmood Sulehri

---

**DEVELOPING THE IT STRATEGY**

- When developing “an overall IT strategy”, the following aspects should be taken into consideration:
  - Key business areas that could benefit from investment in technology
  - Cost
  - Performance criteria
  - Implications for existing workforce
  - Whether Database approach is needed

- Database approach: An approach whereby a pool of related data is shared by multiple application programs; offers significant advantages over traditional file-based approach

by: Bilal Mahmood Sulehri
EXAM QUESTIONS

Smart Industries Limited is using many computer-based applications most of whom have been developed in-house. They are considering to replace them with applications using web based technologies.

Required:
Explain how can the following e–business models assist the company in improving its business:
(a) Business-to-Consumer model.
(b) Business-to-Business model.

(10 marks)
(Summer 08)

by: Bilal Mahmood Sulehri

ANSWER

○ The company can made use of the B2C model in the following way:

○ The company can make basic information of its products available at its website. Such information may include product price, availability, features of the product and any additional charges such as delivery or insurance etc. When such information is available to potential customers in an easy to understand format, it will be easier for them to make decisions and they will be automatically attracted towards company’s website.

○ The company can provide some form of personalization of the website for repeat visits such as welcoming the customer by name or displaying a list of products already reviewed. This would help make the site more customer-friendly and probability of customers’ visiting the company’s website before any related purchase would increase.

○ Providing some incentives to use the website such as loyalty points may help to attract more customers.

by: Bilal Mahmood Sulehri
**ANSWER**

- New customers may be reached, especially those who are not located within traveling distance of the company’s sales outlet.
- When a purchase is made on company’s website, customer information will be stored by the company’s computer system. This information can be used to help provide repeat business for the organization.
- Data can be mined to identify relationship in purchases.
- The company can carry out business on 24 X 7 basis.

**ANSWER**

- **B2B** model can assist the company in improving its performance in the following manner:
  - Managing inventory more efficiently.
  - Suppliers can be given access to stock levels such that when stocks fall below a re-order level, the supplier will automatically send replacement stocks. Thus less employee time will be spent in reviewing stock levels, and replacement stocks will be received immediately when they are required.
  - Self generated e-mails can be used to inform suppliers about new stock requirements.
  - Information concerning stock deliveries and receipts can be sent by Electronic Data Interchange. This will provide time and cost savings.
  - Payment process can be expedited by making payments electronically.
  - Paperless environment.
  - Need to re-enter the data will be reduced.
Electronic commerce, commonly known as e-commerce, refers to the buying and selling of products or services over electronic systems such as the Internet and other computer networks.

Electronic commerce draws on such technologies as electronic funds transfer, supply chain management, Internet marketing, online transaction processing, electronic data interchange (EDI), inventory management systems, and automated data collection systems.

Modern electronic commerce typically uses the World Wide Web at least at one point in the transaction's life-cycle, although it may encompass a wider range of technologies such as e-mail, mobile devices and telephones as well.


by: Bilal Mahmood Sulehri
E-COMMERCE MODELS

- B2C (Business to Consumer)
- B2B (Business to Business)
- B2E (Business to Employee)
- C2C (Consumer to Consumer)
- G2C (Government to Consumer)

by: Bilal Mahmood Sulehri

B2C

- Business to Consumer concentrates to retail or sale side of the e-Commerce. It is commerce between companies and consumers, involves customers gathering information; purchasing physical goods like books or travel or information goods like downloadable digitized material content, such as software, music or electronic books.

- E.g. Amazon.com, Aroma.pk

by: Bilal Mahmood Sulehri
EXAMPLE: B2C

E X A M P L E : B 2 C

EXAMPLE: B2C

EXAMPLE: B2C

EXAMPLE: B2C
**B2C**

- Differences between traditional shopping and B2C.
  - B2C – electronically
  - Location is not an issue
  - 24/7 – 365 days a year
  - B2C - Zero stock

- Disadvantages:
  - Security concerns, e.g. security of credit card information etc.
  - Absence of tangible relationship between seller and distribution channels
  - What you see is (sometimes) not what you get
  - Logistics, shipping and distribution challenges
  - No “touch” or “trial” (as required in several items like clothes)

---

**B2B**

- B2B e-commerce is simply e-commerce between two or more companies.
# B2B

- Differences between traditional business transactions and B2B:
  - B2B – electronically, paperless environment
  - B2B transactions can be completed faster
  - Similar standards (e.g. EDI) should be used for B2B
  - B2B integrates systems and procedure for business transactions

- Disadvantages:
  - Security concerns, (B2B will only thrive in a secure environment)
  - High investment needed for implementation of industry recognized standards
  - Heavily technology driven. Only large companies can adopt B2B due to significant cost involved

- Advantages
  - Timeliness and accuracy of transactions
  - What you see is (sometimes) not what you get

---

# B2E

- Refers to use of technology to handle activities that take place within a business.

- Employees hired are based on various geographical locations. e.g. Telecommuting.

- Collaborative working. Latest example: Google Drive (Google Docs)

- E.g. blogging, writing, software development etc.

- Prerequisites
  - Employee should own a PC/ laptop
  - Fast and secure internet connection

- Consideration
  - Cost of travelling
  - Security of company’s data
  - Sensitivity of company’s data

---

by: Bilal Mahmood Sulehri
C2C

- Exchange of goods and services (including value added information and knowledge) between consumers

Examples

- Forums about specific products or services
- Auctions portals, such as eBay, which allows online real-time bidding on items being sold in the Web
- Hafeezcentre.pk
- Olx.com.pk

Advantages

- Cost and time saving
- Interaction with other consumers (especially before buying a new product)
- Opportunities for businesses due to greater audience

by: Bilal Mahmood Sulehri
G2C

- Governments use internet to stay in touch with citizens.

- Examples
  - FBR.gov.pk
  - SeCP.gov.pk

M-COMMERCE

- Mobile commerce or m-commerce is defined as a process of buying and selling of goods or services through wireless technology (mobile phone)

- There is also increasing amount of services available in m-commerce sector for example:
  - Data or information services (news alerts etc.)
  - Easy Paisa
  - UBL Omni

by: Bilal Mahmood Sulehri
**Electronic Data Interchange (EDI)**

- EDI is a form of computer-to-computer data transfer. For instance instead of sending a customer a paper invoice through the post the data is sent over telecommunications links. This offers savings and benefits to organizations that use it.

- Benefits:
  - It reduces the delays caused by postal paper chains.
  - It avoids the need to re-key data and therefore saves time and reduces errors.
  - It provides the opportunity to reduce administrative costs e.g. the costs associated with the creation, recording and storage of paper documents.
  - It facilitates shorter lead times and reduced stock holdings which allow reduction working capital requirements, (e.g. Just-In-Time policies).
  - It provides the opportunity to improve customer service.

---

**Electronic Cash**

- E-Cash addresses circumstances in which the payer is *not* present at the point of sale or service, but has electronic communications facilities available.

- e.g. is connected to the Internet, or to some other manifestation of the emergent global information infrastructure, such as a cable-TV installation with enhanced capabilities.

- E.g. stored-value cards, e-shopping cards etc.
Kerberos

- Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography.

- Kerberos was created by MIT (Massachusetts Institute of Technology) as a solution to network security problems.

- Kerberos protocol uses strong cryptography so that a client can prove its identity to a server (and vice versa) across an insecure network connection. After a client and server have used Kerberos to prove their identity, they can still encrypt all of their communications to ensure privacy and data integrity as they go about their business.

by: Bilal Mahmood Sulehri
INFORMATION SYSTEMS STRATEGY

- A good starting point for organizations planning to use information systems as a strategic weapon against competition:
  - Develop a partnership, relationship with suppliers and vendors
  - Support and shape changes in traditional business operations
  - Connect various business & users together
  - Allow all employees to access computer
  - Search external databases to obtain data on a competitor’s products and services
  - Revisit the information flow between the home office and field offices, & between headquarters & manufacturing plants and warehouses
  - Have representatives of functional end user groups present on the information steering committee
  - Reengineer the information systems organization
  - Put more focus on lowering the cost of doing business, improving customer service, and cutting the time-to-market of new products and services
  - Help re-engineer business processes
  - Develop a new class of application systems that use existing production data to improve business decisions and, ultimately, customer service

by: Bilal Mahmood Sulehri
INFORMATION SYSTEMS STRATEGY

- Critical success factors:
  - People
  - Process
  - Tools

- IS Strategic Plan: supports an organizational strategic plan. It describes how an organization will manage information and other resources to support the manufacture of products and the delivery of services to its customer base.

- Key components of an IS strategic plan:
  - Mission statement
  - Vision
  - Goals
  - Environmental analysis
  - Strategies
  - Risk assessments
  - Critical success factors

- For strategic planning to succeed, managers must:
  - Commit to and participate in the process
  - Nurture strategic thinking
  - Communicate with all parties
  - Gain staff and client support
  - Develop operational plans

Steering Committee performs the following functions:
- Review the long & short range plans
- Review & approve major acquisitions of hardware & software
- Approve & monitor major projects
- Provide liaison
- Review adequacy of resources and allocation
- Make decisions regarding centralization versus decentralization
- Review and approve plans for outsourcing

Policies: are high level documents

Procedures: Detailed documents

Hiring: (focus on control risks as well)
- Background checks
- Confidentiality agreements
- Employee bonding to protect against losses due to theft
- Conflict of interest agreements
- Non-complete agreements

by: Bilal Mahmood Sulehri
Policies & Procedures

- Employee handbook: should explain all relevant policies and procedures. (relate this to DRP and BCP)

- Well defined promotion policies should be there

- Proper training should be provided on fair & regular basis

- Termination policies should be well defined:
  - Return of all access keys, ID cards and badges to prevent easy physical access.
  - Deletion of assigned logon-ID and passwords to prohibit system access.
  - Notification to other staff and facilities security to increase awareness of the terminated employee’s status.
  - Arrangement of the final pay routines to remove the employee from active payroll files.
  - Performance of a termination interview to gather insight on the employee’s perception of management.
  - Return of all company property

by: Bilal Mahmood Sulehri

---

Policies & Procedures

- Reasons for embarking on outsourcing
  - Reasons for embarking on outsourcing include: ^ A desire to focus on core activities.
  - Pressure on profit margins.
  - Increasing competition that demands cost savings.
  - Flexibility with respect to both organization and structure.

- Third party services
  - Data entry (mainly airlines follow this route).
  - Design and development of new systems
  - Maintenance of existing applications to free in-house staff to develop new applications.
  - Conversion of legacy applications to new platforms. For example, a specialist company may web enable an old application.
  - Operating the help desk or the call center.

- Advantages of outsourcing
  - Commercial outsourcing companies can achieve economies of scale through deployment of reusable component software.
  - Outsourcing vendors are likely to be able to devote more time and focus more effectively and efficiently on a given project than in-house staff.
  - Outsourcing vendors are likely to have more experience with a wider array of problems, issues and techniques than in house staff.
  - The act of developing specifications and contractual agreements for outsourcing services is likely to result in better specification than if developed only by and for in house staff.
  - As vendors are highly sensitive to time consuming diversions and changes, feature creep is substantially less with outsourcing vendors.

by: Bilal Mahmood Sulehri
POLICIES & PROCEDURES

- Disadvantages of outsourcing
  - Costs exceeding customer expectations.
  - Loss of internal IS experience.
  - Loss of control over IS.
  - Vendor failure.
  - Limited product access.
  - Difficulty in reversing or changing outsourced arrangements

- Business Risks from Outsourcing: Business risks from outsourcing are the hidden costs, contract terms not being met, service costs not being competitive over the period of the entire contract, obsolescence of vendor IT systems and the balance of power residing with the vendor. Some of the ways that these risks can be reduced are:
  - By establishing measurable partnership-enacted-shared goals and rewards
  - Utilization of multiple suppliers or withhold a piece of business as an incentive
  - Formation of a cross-functional contract management team
  - Contract performance metrics
  - Periodic competitive reviews and benchmarking
  - Implementation of short-term contracts
  - Address data ownership in the contract

by: Bilal Mahmood Sulehri

IS MANAGEMENT PRACTICES

- The IS auditor must be aware of the various forms outsourcing can take and the associated risks. In general, audit/security concerns of outsourcing include:
  - Contract protection - contract adequately protects the company
  - Audit Rights - right to audit vendor operations
  - Continuity of operations - continued service in the event of a disaster
  - Integrity, confidentiality and availability of company-owned data
  - Personnel - lack of loyalty for customer or disgruntled over outsource arrangement
  - Access control/security administration - vendor controlled
  - Violation reporting and follow up - vendor controlled
  - Change control and testing - vendor controlled
  - Network controls - vendor controlled
  - Performance management - vendor controlled

- IS department should have various logs. E.g.
  - Data entry staff (if present) should keep full details of each batch of work
  - Computer operators should maintain logs of all batch jobs and the time taken to complete them.
  - Back ups, storage of data off-site should be logged
  - Any problems in hardware or software infrastructure should be identified in daily logs.
  - Software application systems may generate their own logs of errors.
  - A security subsystem could maintain detailed logs of who did what and when and also if there were any attempted security violations.

by: Bilal Mahmood Sulehri
IS MANAGEMENT PRACTICES

- Quality management is the means by which IS department based processes are controlled, measured and improved; Areas of control for quality management include:
  - Software development, maintenance and implementation
  - Acquisition of hardware and software
  - Day-to-day operations
  - Security
  - Human resource management
  - General administration

- ISO 9126
  - Functionality
  - Reliability
  - Usability
  - Efficiency
  - Maintainability
  - Portability

IS MANAGEMENT PRACTICES

- The capability maturity model defines five levels of organizational maturity and the software quality processes associated with each of the levels.

<table>
<thead>
<tr>
<th>LEVEL</th>
<th>CHARACTERISTICS</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Best practice pursued</td>
</tr>
<tr>
<td>5</td>
<td>Continuous process improvement</td>
</tr>
<tr>
<td>4</td>
<td>Quantitative quality goals</td>
</tr>
<tr>
<td>4</td>
<td>Quality and productivity measured</td>
</tr>
<tr>
<td>3</td>
<td>Processes tailored to specific projects</td>
</tr>
<tr>
<td>3</td>
<td>Documented processes</td>
</tr>
<tr>
<td>2</td>
<td>Basic project management controls</td>
</tr>
<tr>
<td>2</td>
<td>Disciplined processes</td>
</tr>
<tr>
<td>1</td>
<td>Reliance on key personnel</td>
</tr>
<tr>
<td>1</td>
<td>Unstable software environment</td>
</tr>
</tbody>
</table>

by: Bilal Mahmood Sulehri
IS ORGANIZATION STRUCTURE

- Organizational and management controls within the IPF encompass the following:
  - Sound human resource policies and management practices.
  - Separation of duties among the information processing environment and other organizational environments or functions.
  - Separation of duties within the information processing environment.
  - Methods to assess effective and efficient operations.

- An information systems department may be headed by an IS director (sometimes called the Chief Information Officer – CIO). The following positions in the IS department may report to this individual:
  - Control group
  - Systems Development Manager
  - Help Desk
  - End User
  - End-User Support Manager
  - Data Management
  - Database Administrator
  - Technical Support Manager
  - Security Administrator
  - Systems Administrator
  - Network Manager/ Administrator
  - Operations Manager
  - Quality Assurance Manager

by: Bilal Mahmood Sulehri

IS ORGANIZATION STRUCTURE

- Data Entry staff performs the following tasks:
  - Receives source documents from various departments and ensures proper safekeeping of such until processing is complete and source documents and output are returned.
  - Prepares batches of source documents with accurate control totals.
  - Schedules and sets up the jobs to process input.
  - Verifies, logs, and distributes output to the appropriate department with special care for confidential information.

- The security administrator’s functions usually include:
  - Maintaining security and confidentiality over the issuance and maintenance of authorized user IDs and passwords.
  - Monitoring security violations and taking corrective action to ensure that adequate security is provided.
  - Periodically reviewing and evaluating the security policy and suggesting necessary changes to management.
  - Preparing and monitoring the security awareness program for all employees.
  - Testing the security architecture to evaluate the security strengths and to detect possible threats.
  - Maintaining access rules to data and other IT resources.

by: Bilal Mahmood Sulehri
IS ORGANIZATION STRUCTURE

- Quality Assurance: The quality group usually performs two distinct tasks, namely:
  - Quality assurance (QA) and quality control (QC)
    - Quality Assurance helps the IS department to ensure that the personnel are following prescribed quality processes.
    - Quality Control is responsible for conducting tests or reviews to verify and ensure that the software is free from defects and meets user expectations.

- The database administrator (DBA) defines and maintains the data structures in the corporate database system. DBA's role includes:
  - Specifying physical (computer orientated) data definition.
  - Changing physical data definition to improve performance.
  - Selecting and implementing database optimization tools.
  - Testing and evaluating programmer and optimization tools.
  - Answering programmer queries and educating programmers in the database structures.
  - Implementing database definition controls, access controls, update controls and concurrency controls.
  - Monitoring database usage, collecting performance statistics and tuning the database.
  - Defining and initiating back up and recovery procedures.

- The IS department must exercise close control over database administration through:
  - Separation of duties
  - Management approval of DBA activities.
  - Supervisor review of access logs.
  - Detective controls over the use of database tools.

by: Bilal Mahmood Sulehri

IS ORGANIZATION STRUCTURE

<table>
<thead>
<tr>
<th>Control Group</th>
<th>Systems Analyst</th>
<th>App Prgm</th>
<th>Data Entry</th>
<th>Comp Oprtr</th>
<th>DB Admin</th>
<th>Sec Admin</th>
<th>Tape Librnr</th>
<th>Sys Program</th>
<th>Qty Assn</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Group</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Systems Analyst</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Programming</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Entry</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Computer Operator</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Database Administrator</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Administrator</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tape Librarian</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Systems Programming</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Quality Assurance</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

X-functions should not be combined

by: Bilal Mahmood Sulehri
REVIEW OF IT PLANNING/ STRATEGY

- While many conditions exist which are of concern to the IS Auditor when auditing the information processing facility (IPF), some of the more significant indicators of potential problems include:
  - Unfavorable end user attitudes
  - Excessive costs
  - Budget overruns
  - Late projects
  - High-staff turnover
  - Inexperienced staff
  - Frequent hardware/software errors
  - Excessive backlog of user requests
  - Slow computer response time
  - Numerous aborted or suspended development projects
  - Unsupported or unauthorized hardware/software purchases
  - Frequent hardware/software upgrades
  - Extensive exception reports
  - Exception reports which were not followed up on
  - Poor motivation
  - Lack of succession plans
  - Reliance on one or two key personnel

by: Bilal Mahmood Sulehri

REVIEW OF IT PLANNING/ STRATEGY

- The following documents should be reviewed (authorization, up-to-date)
  - IT strategies, plans and budgets
  - Security policy documentation
  - Organizational/ functional charts
  - Job descriptions
  - Steering committee reports
  - System development and program
  - Operations procedures
  - Human resource manuals

- IS auditor should interview and observe personnel to assess their duties
  - Actual functions
  - Security awareness
  - Reporting relationships

- Reviewing Contractual Commitments
  - Development of contract requirements
  - Contract bidding process
  - Contract selection process
  - Contract acceptance
  - Contract maintenance
  - Contract compliance

by: Bilal Mahmood Sulehri
SERVICE LEVEL AGREEMENTS (SLA)

- Service Level Agreement (SLA) is a written contract between a provider of a service and the consumer of the service. The purpose of the SLA is to establish measurable targets of performance with the objective of achieving a common understanding of the nature of and levels of service required.

- IT management should have formal SLAs with all of their IT customers because these contracts provide:
  - Defined levels of service
  - Accountability for the service
  - Evaluation criteria and a basis for improvement
  - Performance criteria
  - Methods and processes of delivering the service
  - A method for communicating service expectations and actual performance;
  - A basis for costing IT services to their customers.

- The agreement defines the responsibilities of both parties and should encompass the following aspects:
  - Availability
  - Reliability
  - Performance
  - Support
  - Business continuity planning
  - Security
  - Service charges
  - Capacity for growth
  - Change management
  - Penalties for non-delivery

by: Bilal Mahmood Sulehri

SERVICE LEVEL AGREEMENTS (SLA)

- IT management should establish a benchmark for measuring performance to meet the agreed-on quality and quantity of service. Common pitfalls which can be possible in such agreements are:
  - Performance criteria are not specific
  - Customer obligations are not adequately defined
  - Service levels are not reviewed regularly
  - Performance is not monitored on a regular basis
  - Performance expectations are unrealistic
  - Method of delivery is not agreed on
  - Requirements are not adequately defined

- Benefits of SLAs:
  - Delivery and support of IT services meets the service levels defined in the SLA.
  - IT customer expectations can be managed efficiently because the SLA provides an effective communication and performance measurement tool.
  - Definitions of responsibilities, response times, volumes, charges, etc., are clear, objective and understood by all parties involved.
  - Service levels should improve over time.

by: Bilal Mahmood Sulehri
SUPPLY CHAIN MANAGEMENT

WHAT IS SCM

- A product or service is delivered to the ultimate consumer through a complex interaction of several companies on the way, i.e. through supply chain.

- Supply Chain Management is concerned with the total management of the supply chain.

- Supply chain management (SCM) is the management of a network of interconnected businesses involved in the provision of product and service packages required by the end customers in a supply chain. Supply chain management spans all movement and storage of raw materials, work-in-process inventory, and finished goods from point of origin to point of consumption.

- Another definition is provided by the APICS Dictionary when it defines SCM as the "design, planning, execution, control, and monitoring of supply chain activities with the objective of creating net value, building a competitive infrastructure, leveraging worldwide logistics, synchronizing supply with demand and measuring performance globally."

by: Bilal Mahmood Sulehri
SUPPLY CHAIN MANAGEMENT

Objective of SCM: To provide the highest possible level of customer service at the lowest cost

Successful growth companies pursue (one or more of) the following strategic growth opportunities:
- Customer Franchise Management
- New Products/ Services Development Strategy
- Channel Management

Universal underlying pre-requisites for growth:
- Value: Comparatively superior value as defined by your customers
- Economics: Comparatively superior economics across the value chain
- Execution: Consistently superior strategy execution via organizational alignment

SUPPLY CHAIN MANAGEMENT

Universal success factors for a supply chain:
- Market driven customer service strategy
- Optimum logistics cost and investment
- Logistics MIS
- Logistics organizational structure

Market driven customer service strategy
- Product availability (order fill)
- Length of order cycle time
- Consistency of order cycle time
- Invoice/ billing procedures/ accuracy
- Information request responsiveness
- Flexibility in resolving problems
- Distance to suppliers warehouse
- Special customer requests
- Frequency of damaged goods
- Emergency coverage
- On-time delivery

by: Bilal Mahmood Sulehri
WHAT IS ERP?

- ERP is an industry term for integrated, multi-module application software packages that are designed to serve and support multiple business functions.

- An ERP System can include software for manufacturing, order entry, accounts receivable and payable, general ledger, purchasing, warehousing, transportation and human resources.

- Examples:
  - Oracle
  - SAP
  - Microsoft Dynamics
  - Sidat Hyder Financials
  - Hassan Naeem Financials

by: Bilal Mahmood Sulehri
WHY ERP MATTERS FOR A CA?

○ CA as a consultant:
  • Implementing ERP one of the largest drivers of growth
  • A CA plays major role in implementation of an ERP project as a consultant

○ CA as an auditor
  • A lot of clients have ERP solutions implemented
  • Ensure that internal controls and checks are maintained consistently
  • Ensure that provisions of tax etc. have been incorporated in the system
  • Ensure that IFRSs are consistently followed across the company
  • Improves the quality of reporting

by: Bilal Mahmood Sulehri

WHY ERP MATTERS FOR A CA?

○ CA as an advisor
  • An advisor of a company must be aware of ERP solutions and their implications in order to advise a company.

○ CA as a manager
  • CA working as a manager in a company will be able to achieve their targets and goals by proper utilization of ERP systems in their organization
  • CA working as a manager will need to co-ordinate with the technical staff in various phases during development and implementation of an ERP

by: Bilal Mahmood Sulehri
BRIEF HISTORY OF ERP

1960s
• Inventory Control

1970s
• Material Resource Planning (MRP)

1980s
• Manufacturing Resource Planning (MRP-II)

1990s
• MRP-II Extended

2000s
• ERP

by: Bilal Mahmood Sulehri

WHY ERP IS NEEDED BY BUSINESSES

Because businesses are subject to the following demands:
• Aggressive cost control initiatives
• Need to analyze costs/revenues on a product or customer basis
• Flexibility to respond to changing business requirements
• More informed management decision making
• Changing in ways of doing business

Systems used to fulfill the aforementioned demands:
• Management Information System (MIS)
• Executive Information System (EIS)
• Enterprise Wide System (EWS)
• Material Resource Planning (MRP)
• Manufacturing Resource Planning (MRP II)
• Money Resource Planning (MRP III)

by: Bilal Mahmood Sulehri
FEATURES OF ERP

Some major features of ERP are as follows:
- Company-wide integrated information system
- Performance of core corporate activities & increases customer satisfaction
- Bridges the information gap across the organization
- Complete integration of system (across departments and group of companies)
- Better project management
- Utilization of latest technology for betterment of business
- Eliminate problems as material shortages, quality problems, delivery delays
- Opportunity of continuous refinement and improvement of business processes

by: Bilal Mahmood Sulehri

COMPONENTS OF ERP

Some components (modules) of ERP are as follows:
- Sales and marketing
- Scheduling
- Material requirement planning
- Capacity requirement planning
- Purchasing
- Inventory management
- Shop floor control
- Accounts payable/ receivable
- Logistics
- Asset management
- Financial Accounting
- Budgeting
- Production

by: Bilal Mahmood Sulehri
BUSINESS PROCESS RE-ENGINEERING

- Business Process Re-Engineering involves the following steps:
  - Study the current system
  - Design and develop a new system
  - Define process, organization structure and procedure
  - Develop & customize the software
  - Train people
  - Implement new system
  - Conduct a post-implementation review

by: Bilal Mahmood Sulehri

ERP

- Following points should be considered while selecting an ERP solution:
  - All functional aspects of the business are fully covered
  - Business functions and processes are fully integrated
  - Latest IT trends are covered
  - Vendor has the ability to customize, train and implement
  - Business can absorb the cost
  - ROI is optimum

- Major phases in implementation of ERP
  i. Detailed discussion phase
  ii. Design and customization phase
  iii. Implementation phase
  iv. Production phase

by: Bilal Mahmood Sulehri
BENEFITS OF ERP

- Increased control over invoicing and payment
- Reduce usage of paper
- Improved timeliness of information
- Improved control of cost
- Faster response and follow up on customers
- Efficient cash collection
- Better monitoring and quicker resolution of queries
- Improved business processes – competitive advantage
- Unified customer database
- Improved international operations
- Better decisions due to availability of structured data
- Better projections due to access on previous trends
- Better management oversight
- Improved reporting

by: Bilal Mahmood Sulehri
Customer Relationship Management (CRM) is a widely implemented model for managing a company's interactions with customers, clients, and sales prospects. It involves using technology to organize, automate, and synchronize business processes—principally sales activities, but also those for marketing, customer service, and technical support.

The overall goals are to find, attract, and win new clients; nurture and retain those the company already has; entice former clients back into the fold; and reduce the costs of marketing and client service.
CRM can be useful for a business to:

- Track orders
- Pinpoint buying behavior
- Build compelling promotions
- Locate cross-selling and up-selling opportunities
- Build customer care from inside your company

Considerations for selecting a CRM solution:

- Who are your customers?
- How many people need to work with your CRM tools?
- What roles do they have in the company?
- How does your business receive orders?
- Does your inventory allow for significant cross-selling/up-selling

by: Bilal Mahmood Sulehri
Some of the benefits of using CRM tools are as follows:
- Faster response time
- Increased efficiency
- Increased marketing opportunities
- Insight into customers needs
- Enhanced customer satisfaction

Benefits of using online collaboration tools:
- Increase the efficiency
- Boost turnaround time
- Lower costs
- Streamline project management
- Ensure client confidentiality

by: Bilal Mahmood Sulehri
SALES FORCE AUTOMATION

WHAT IS SFA

- Functions of the Sales team are finding, acquiring and maintaining customers.

- SFA: Sales Force Automation

- Sales force management systems are information systems used in CRM marketing and management that help automate some sales and sales force management functions. They are often combined with a marketing information system, in which case they are often called customer relationship management (CRM) systems.

- SFA use technology to reduce administrative work and increase sales team productivity.

by: Bilal Mahmood Sulehri
**Benefits of SFA**

- Benefits of implementing a (internet based) sales force management system or Sales Force Automation are as follows:
  - Streamline sales processes
  - Boost salesperson knowledge
  - Enhance collaborative selling
  - Improve customer relationships
  - Reduce quote times
  - Integrate sales with other company data
  - Increase sales force morale

**Other Benefits**

- Other benefits of SFA include:
  - Unexpected new knowledge. Information can be presented in ways which were not possible before, hence revealing new insight.
  - Validation of sales for marketing purposes
  - The ability for users to bring up a list of leads, search and sort in a number of different ways
  - Improved account planning by attaching account plans, so the entire selling team can see the broader context of the account
**CONSIDERATIONS**

- Before selecting a SFA, following factors should be considered:
  - Well defined sales process
  - Selected tool should be compatible with the business
  - A cross-functional team for selection and implementation of SFA
  - Clearly articulated value proposition (of the tool)
  - Unswerving commitment from all the executives
  - Win-win-win situation for the sales force, delivery teams and the management
  - SFA designed to help people manage their work and get organized. Allowing them to spend more time with customers
  - Pending opportunities (leads) should be a focus point while selecting/developing SFA
  - Allow easy to create, self serving management reports. Ability to consolidate and break reports in various ways

by: Bilal Mahmood Sulehri
INFORMATION SYSTEMS
AUDIT, PROCESS AND CONTROLS

WHY CONTROLS?

- Computers are everywhere
- Access to data is easier than ever
- Data abuse is easier

- Reasons for establishing a function to examine controls over computer-based data processing:
  - Organizational costs of data loss
  - Costs of incorrect decision making
  - Costs of computer abuse
  - Value of hardware, software, personnel
  - High costs of computer error
  - Maintenance of privacy
  - Controlled evolution of computer use

by: Bilal Mahmood Sulehri
## COMPUTER ABUSE

<table>
<thead>
<tr>
<th>Type of Abuse</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hacking</td>
<td>A person gains unauthorized access to a computer system</td>
</tr>
<tr>
<td>Viruses</td>
<td>Viruses are programs that attach themselves to executable files, system areas on diskettes or data files that contain macros. They are designed to achieve two objectives: replicate and disruption</td>
</tr>
<tr>
<td>Illegal physical access</td>
<td>A person gains unauthorized physical access to computer facilities</td>
</tr>
<tr>
<td>Abuse of privileges</td>
<td>A person uses privileges they have been assigned for unauthorized purposes</td>
</tr>
</tbody>
</table>

by: Bilal Mahmood Sulehri

## CONSEQUENCES OF COMPUTER ABUSE

<table>
<thead>
<tr>
<th>Consequences of Abuse</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destruction of assets</td>
<td>H/w, s/w, data facilities</td>
</tr>
<tr>
<td>Theft of assets</td>
<td>H/w, s/w, data, documentation</td>
</tr>
<tr>
<td>Modification of assets</td>
<td>Unauthorized modification</td>
</tr>
<tr>
<td>Privacy violations</td>
<td>Privacy of data can be compromised</td>
</tr>
<tr>
<td>Disruption of operations</td>
<td>Operations can cease</td>
</tr>
<tr>
<td>Unauthorized use of assets</td>
<td>H/w, s/w, data facilities etc. can be used in an unauthorized manner</td>
</tr>
<tr>
<td>Physical harm to personnel</td>
<td>Personnel can suffer physical harm due to attacks and industrial espionage</td>
</tr>
</tbody>
</table>

by: Bilal Mahmood Sulehri
**IS AUDITING**

- Def: Information systems auditing is a process of collecting and evaluating evidence to determine whether a computer system safeguards assets, maintains data integrity, allows organizational goals to be achieved effectively, and uses resources efficiently.

- IS Auditing helps organizations to achieve four major objectives
  - Improved safeguarding of assets
  - Improved data security
  - Improved system effectiveness
  - Improved system efficiency

---

**OBJECTIVES OF IS AUDITING**

- Asset Safeguarding
  - H/w, s/w, facilities, people (knowledge), data files, documentation

- Data Integrity
  - It is a state implying data has certain attributes: completeness, soundness, purity and veracity

- System Effectiveness
  - Effectiveness auditing: check whether the system is achieving its stated objectives

- System Efficiency
  - An efficient IS uses minimum resources to achieve its required objective
AUDIT CHARTER

- Every organization should have an approved charter (mandate, mission statement) describing audit function’s purpose, authority, scope and responsibilities. E.g.

- Purpose: IS auditing is an independent appraisal activity established to conduct computer systems and operations reviews and to report findings and recommendations to management and others.

- Authority: In carrying out its duties, the audit function shall have full, free and unrestricted access to all of the organization's activities, functions, record, property and personnel necessary for executing agreed audit plans.

- Scope & responsibilities: An IS Audit function should perform assurance to management that the controls which govern computer systems and operations are properly conceived and effectively administered.

by: Bilal Mahmood Sulehri

AUDITORS

- Internal Auditor: Employed within the organization. Acts as a control mechanism to:
  - Ensure adequate internal control
  - Review the reliability of records
  - Prevent & detect fraud
  - Carry out statutory duties (if applicable)
  - Monitor the reporting procedures
  - Provide advice as how to improve performance of organization

- Assignments by internal auditors:
  - Systems reviews
  - Special investigations
  - Consultancy
  - Efficiency/ cost effectiveness audits

- External Auditor: Independent examination, express an opinion. Reports to: Owners, potential investors, suppliers of credit.

by: Bilal Mahmood Sulehri
AUDITS

- Classification of audits:
  - Financial Audits
  - Operational Audits
  - Integrated Audits
  - Administrative Audits
  - Information System Audits

- Audit methodology is a set of documented audit procedures designed to achieve planned audit objectives.
  - Audit subject
  - Audit objective
  - Audit scope
  - Pre-audit planning
  - Audit procedures & steps for data gathering
  - Procedures for evaluating the test or review results
  - Procedures for communication with management
  - Audit report preparation

by: Bilal Mahmood Sulehri

AUDITS

- Categories of audit risk:
  - Inherent risk
  - Control risk
  - Detection risk
  - Overall audit risk

- Types of testing:
  - Substantive testing
  - Compliance testing

- Determinants for evaluating the reliability of audit evidence include:
  - Independence of provider of evidence
  - Qualification of the individual providing information or evidence
  - Objectivity of the evidence

by: Bilal Mahmood Sulehri
IS AUDIT REPORT

- Structure & content of IS audit report:
  - Introduction to report
  - IS auditor’s overall conclusion and opinion
  - Communication of reservations or qualifications
  - Detailed audit findings & recommendations
  - Variety of findings
  - Summary report
- IS auditor should recognize that management may not be able to implement all the recommendations immediately.
- IS auditor should discuss the recommendations and any planned implementation dates during the process of releasing the audit report.

- Following presentation techniques can be used
  - Executive summary
  - Visual presentation

CAATs

- CAAT: Computer Assisted Audit Techniques

- Application of CAATs:
  - Test data generators
  - Expert systems
  - Standard utilities
  - Software library packages
  - Integrated test facilities
  - Snapshot
  - System control audit review file
  - Specialized audit software
ADVANTAGES OF CAATs

- Greater productivity through:
  - Reduced audit cycle
  - Automated repetitive tasks
  - Focused time on critical functions
  - Simplified documentation
  - Improved planning process

- Value addition by:
  - Providing timely results
  - Recuperating lost revenue
  - Quantifying impact of given conditions
  - Offering creative and detailed analysis

Reducing costs by:
- Lowering EDP (electronic data processing) costs
- Minimizing software maintenance costs
- Reducing travel costs

Improved quality of audits, due to:
- Audit 100% of data files
- Standardized audit methodologies
- Verifying audit procedures
- Assure integrity of analysis

Independence from IS because of:
- Simplification of data access
- Isolation of exceptions independently
- Elimination of the need to sample

by: Bilal Mahmood Sulehri
ADVANTAGES OF CAATs

- Reducing audit delivery time:
  - Minimize waiting time required for gathering information
  - Accelerate the identification of exceptions
  - Simplifying the preparation of working papers
  - Automate the entire analysis

- Corporate benefits:
  - Reduce today’s risk
  - Prepare for tomorrow’s risk
  - Recover audit investment
  - More efficient
  - More effective
  - Optimized use of resources
  - Real change in audit image

by: Bilal Mahmood Sulehri

ADVANTAGES OF CAATs

- Personal benefits to the auditor:
  - Independence
  - Renewed focus on audit
  - Elimination of repetitive work
  - Greater creativity
  - Reduced audit risk

- Audit benefits – Today’s technology
  - Exception reporting
  - Control analysis
  - Statistical sampling
  - Immediate results
  - Easy to use: PC based
  - Highly flexible
  - Extremely fast
  - More than just analysis

by: Bilal Mahmood Sulehri
DISADVANTAGES OF CAATs

- Training requirements of most of the CAATs are extensive.

- Even if use of the CAATs is mastered, the techniques for selecting the transaction for audit depend upon the auditor’s creativity, experience & understanding of audit area.

- Some CAATs are so general that customizing them for specific use might be difficult.

- Extracting the transaction data in the format required by CAATs for auditing, where application is running across multiple platforms, might require the auditor to possess high IT skills.

by: Bilal Mahmood Sulehri

DOCUMENTATION OF CAATs

- When developing CAATs, the following documentation should be retained:
  - Commented program listings
  - Flowcharts
  - Sample reports
  - Record and file layouts
  - Field definitions
  - Operating instructions
  - Description of applicable source documents

- The CAATs documentation should be referenced to audit program and clearly identify the procedures and objectives being served.

by: Bilal Mahmood Sulehri
CAATs

- Some leading CAATs:
  - ACL
  - IDEA
  - Audimation
  - Automated Audit Services
  - AutoAudit2001
  - Magique

- Considerations for selection of CAATs:
  - Ease of use
  - Capacity to handle data
  - Efficiency of analysis
  - Level of training required
  - Effectiveness in preventing and/or detecting frauds
  - Cost and licensing structure

by: Bilal Mahmood Sulehri

CAATs

- Use of CAATs in banks:
  - Interest earned on advances
  - Interest paid on deposits
  - Recover of commission and income from non-fund businesses
  - Scrutiny of large value transactions in cash credit accounts
  - Transactions in dormant accounts

by: Bilal Mahmood Sulehri
INFORMATION SYSTEMS UNDER DEVELOPMENT

SDLC

- SDLC: System Development Life Cycle
- Phases of SDLC:
  1. Systems planning (feasibility)
  2. Systems analysis (requirement definition)
  3. Systems design
  4. Systems development
  5. Systems implementation
  6. Systems operation & maintenance

by: Bilal Mahmood Sulehri
SYSTEMS PLANNING

- Objective: To define the problem

- It has the following steps:
  1. Define a time frame for which the solution is required
  2. Determine an optimum alternative/solution
  3. Determine if an existing system can correct the situation with slight or no modifications
  4. Determine if a vendor product offers a solution to the problem
  5. Determine the approximate cost to develop the system
  6. Determine if the solution fits the business strategy

by: Bilal Mahmood Sulehri

SYSTEMS ANALYSIS

- Objective: To conduct analysis and define business and system requirements

- It is concerned with:
  - Identifying and specifying the requirements of the system
  - Descriptions of what a system should do
  - How users will interact with a system
  - Conditions under which a system will operate
  - The information criteria the system should meet

by: Bilal Mahmood Sulehri
SYSTEMS DESIGN

- Objective: Develop detailed system requirements

- It has the following steps:
  1. Identifying the purpose and major functions of the systems and subsystems
  2. Determining system inputs and outputs
  3. Evaluating the necessary processing functions
  4. Developing system justification and processing alternatives
  5. Defining control, security and audit requirements

- Following are developed during this phase:
  - Program flows
  - Screen flows
  - Job flows
  - Test plans

by: Bilal Mahmood Sulehri

---

SYSTEMS DESIGN

- Key design phase activities:
  - Developing system flowcharts
  - Define applications through a series of data and process flow diagrams
  - Determining processing steps
  - Determining data file or database system file design
  - Preparing program specifications for the various types of requirements or information criteria defined
  - Developing test plans for the various levels of testing:
    - Unit (program)
    - Subsystem (module)
    - Integration (system)
    - Interface with other system
    - Loading and initializing files
    - Security, backup and recovery
  - Developing data conversion plans to convert data and manual procedures from the old system to the new system

by: Bilal Mahmood Sulehri
SYSTEMS DEVELOPMENT

- Objective: To develop computer programs and to conduct testing

- Key activities performed in this include:
  - Coding & developing
  - Debugging & testing
  - Convert data from old systems to use in new systems (programs)
  - Create user procedures to handle transition to the new system
  - Training
  - Ensuring modifications are documented and applied accurately

by: Bilal Mahmood Sulehri

SYSTEMS IMPLEMENTATION

- Objective: To develop user reference and training manuals & train users.

- Steps necessary for successful data conversion are:
  - Determining what data should be converted manually & automatically
  - Performing necessary data cleansing ahead of converting
  - Identifying the methods to be used to verify the conversion
  - Establishing the parameters of a successful conversion
  - Scheduling the sequence of conversion links
  - Designing audit trail reports to document the conversion
  - Designing exception reports (to record unsuccessful conversions)
  - Developing and testing conversion programs, including functionality and performance
  - Performing one or more conversion dress rehearsals
  - Running the actual conversion with all necessary personnel onsite or at least able to be contacted

by: Bilal Mahmood Sulehri
SYSTEMS OPERATION & MAINTENANCE

- Objective: To run the final program with actual data, i.e. getting system “Live”

- Objectives of a post-implementation review:
  - Assess the adequacy of the system
    - Does the system meet its objectives?
    - Have access controls been adequately defined and implemented?
  - Evaluate the project cost benefit or ROI
  - Develop a recommendation addressing system’s inadequacies
  - Develop a plan for implementing recommendations
  - Assess the development project process:
    - Were the chosen methodologies, standards and techniques followed?
    - Were appropriate project management techniques used?

STRENGTH & WEAKNESSES OF SDLC

<table>
<thead>
<tr>
<th>STRENGTHS</th>
<th>WEAKNESSES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control.</td>
<td>Increased development time.</td>
</tr>
<tr>
<td>Monitor large projects.</td>
<td>Increased development cost.</td>
</tr>
<tr>
<td>Detailed steps.</td>
<td>Systems must be defined up front.</td>
</tr>
<tr>
<td>Evaluate costs and completion targets.</td>
<td>Rigidity.</td>
</tr>
<tr>
<td>Documentation.</td>
<td>Hard to estimate costs, project overruns.</td>
</tr>
<tr>
<td>Well defined user input.</td>
<td>User input is sometimes limited.</td>
</tr>
<tr>
<td>Ease of maintenance.</td>
<td></td>
</tr>
<tr>
<td>Development and design standards.</td>
<td></td>
</tr>
<tr>
<td>Tolerates changes in MIS staffing.</td>
<td></td>
</tr>
</tbody>
</table>
TESTING

- Testing is the part of the development process that verifies & validates that a program, subsystem or application performs the functions for which it has been designed.

- Elements of software testing process
  - Test plan: identifies the specific portions of the system to be tested. It has two approaches
    - Bottom up: begin testing of modules and work upwards
    - Top down: follow the opposite path from above
  - Conduct & report test results
  - Address outstanding issues

- Testing methods
  - Unit testing
  - Interface or integration testing
  - System testing
  - Final Acceptance testing

<table>
<thead>
<tr>
<th>Testing Methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recovery testing</td>
</tr>
<tr>
<td>Security testing</td>
</tr>
<tr>
<td>Stress/ Volume testing</td>
</tr>
<tr>
<td>Performance testing</td>
</tr>
</tbody>
</table>

by: Bilal Mahmood Sulehri

OTHER TYPES OF TESTING

- Alpha & beta testing: performed by users within an organization and outside an organization respectively e.g. as in Windows

- Pilot testing: A preliminary test focusing on specific and predetermined aspects of a system

- Whitebox testing: Input-Process-Output

- Blackbox testing: Input--Output

- Function/ validation testing: test functionality of the system

- Regression testing: rerunning specific portions to ensure that changes have not introduced new errors

- Parallel testing: old & new systems run together

- Sociability: how the new system will effect the existing systems

by: Bilal Mahmood Sulehri
ALTERNATE DEVELOPMENT METHODS

- Data-Oriented System Development (DOSD): Focuses on & recognizes the need for management & staff to have access to data to facilitate & support decisions (i.e. focus on the need for information only)

- Object-Oriented System Development (OOSD): Employs solution specification and modeling. Following applications use OOSD
  - Web applications
  - E-business apps
  - Computer-Aided Software Engineering (CASE)
  - Office automation for email and work orders
  - Computer-Aided Manufacturing (CAM)

- Advantages of using OOSD
  - Manage unrestricted variety of data types
  - Means to model complex relationships
  - Capacity to meet demands of a changing environment
  - Object oriented models can be manipulated easily by the user
  - Increased efficiency in programming through the re-use of elements of logic
  - Allow a user or app to access only needed information

by: Bilal Mahmood Sulehri

ALTERNATE DEVELOPMENT METHODS

- Prototyping: Heuristic development. Process of creating a system through control trial and error. Two basic modes
  - Build the model to create design & then create the actual system
  - Gradually build the actual system that will operate in production

- Rapid Application Development (RAD): Using a series of proven app development techniques, within a well-defined methodology. Including use of
  - Small, well-trained dev teams
  - Evolutionary prototypes
  - Integrated power tools
  - A central repository
  - Interactive requirements and design workshops
  - Rigid limits on development time frames

- RAD has 4 stages
  - Concept definition
  - Functional design
  - Development stage
  - Deployment stage

by: Bilal Mahmood Sulehri
ALTERNATE DEVELOPMENT METHODS

- Agile development: Family of similar development processes that espouse the non-traditional ways of developing complex systems. These have a number of characteristics:
  - Use of small, time-boxed projects or iterations
  - Re-planning the project at the end of each iteration
  - Relatively greater reliance on tacit knowledge i.e. the knowledge in people's heads
  - A heavy influence on mechanisms to effectively disseminate tacit knowledge and promote teamwork
  - At least some of the agile methods stipulate pair-wise programming i.e. two persons code same part of the system
  - Change in the role of the project manager from a manager to a facilitator

- Re-engineering: updating an existing system by extracting and reusing design & program components

- Reverse engineering: Taking apart an app or software or a product in order to see how it functions & use that information to develop a similar system. Major advantages are:
  - Faster development & reduced SDLC duration
  - Creation of an improved system using the reverse-engineered app's drawbacks

by: Bilal Mahmood Sulehri

ALTERNATE DEVELOPMENT METHODS

- Reverse Eng: The IS Auditor should be aware of the following risks:
  - Software license agreements prohibit this
  - Decompilers are relatively new tools whose functions depend on many factors

- Structured analysis: In an SA, a developer would want to do the following:
  - Develop system context diagrams
  - Perform hierarchical data flow/ control flow decomposition
  - Develop control transformations
  - Develop mini-specifications
  - Develop data dictionaries
  - Define all external events
  - Define single transformation DFD from each external event

<table>
<thead>
<tr>
<th>Strengths</th>
<th>Weaknesses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Addresses user concerns quickly</td>
<td>Weak solution representation</td>
</tr>
<tr>
<td>More applicable to problem-oriented analysis than design</td>
<td>Doesn't address the issue of structured system into concurrent tasks</td>
</tr>
<tr>
<td>Supports CASE tools</td>
<td></td>
</tr>
</tbody>
</table>
**RISK OF INADEQUATE SDLC**

<table>
<thead>
<tr>
<th>Risk</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inadequate management of the SDLC</td>
<td>Develop IS plans, testing etc.</td>
</tr>
<tr>
<td>User requirements may not be met</td>
<td>Involve users while developing</td>
</tr>
<tr>
<td>Excessive costs or cost overruns</td>
<td>Develop long &amp; short term IS plans, cost estimates in detail etc.</td>
</tr>
<tr>
<td>Incompatibility between systems</td>
<td>Develop data &amp; info architecture models</td>
</tr>
<tr>
<td></td>
<td>Develop systems using open systems</td>
</tr>
<tr>
<td>Excessive delays while developing &amp; maintaining systems</td>
<td>Involve development &amp; maintenance staff while preparing estimates</td>
</tr>
<tr>
<td>Inadequate resources to develop or maintain computer systems</td>
<td>Cost-benefit analysis</td>
</tr>
<tr>
<td>Inadequate &amp; ineffective controls over the system development and/ or maintenance processes</td>
<td>Install management oversight reviews</td>
</tr>
</tbody>
</table>

**SOFTWARE PACKAGE ACQUISITION PROCESS**

1. Solicitation of proposals
2. Proposal evaluation
3. System walkthrough
4. Vendor evaluation
5. Vendor suitability evaluation
6. The vendor review
7. Vendor presentations
8. On-site visits to package users
9. Support evaluation
10. Cost/ Benefit analysis
11. Final package selection
   - Opportunity cost
   - Feature accounting
SOFTWARE PACKAGE ACQUISITION PROCESS

- Some of the deciding factors in acquiring & using purchased software packages, compared to in-house development include:
  - Lower cost to acquire & implement
  - Less time to install the package
  - Limited IS staff to develop & maintain systems in-house
  - Lack of requisite computer skills among the IS staff

- What can go-wrong in vendor developed software
  - May not have adequate built-in usability, security & maintainability features
  - May not have adequate transaction processing audit trails
  - May not have adequate internal program processing (automated) controls
  - Vendor supplied documentation may not be adequate, complete & clear
  - Vendor might provide only the names of satisfied customers not the disgruntled ones
  - System installation & implementation may take longer than planned due to lack of familiarity with the system by end users due to poor service & support from vendor
  - Limited vendor liability

IS MAINTENANCE

- System maintenance practices refer primarily to the process of managing change to application systems while maintaining the integrity of both the production source & executable source

- System maintenance controls refer to the process of modifying application programs, based on organizational needs, while maintaining the integrity of both the production source & executable code

- Change management process: No change to system without justification including cost-benefit analysis.

- The primary purpose of library control software is to:
  - Prohibiting programmers from accessing production source & object libraries
  - Prohibiting batch program updating
  - Require the control group or operator to release source code and place it in the program library
  - Require the programmer to turn over changed source code to the control group or operator who updates the object library or programmer testing
  - Require the control group or operator to update the object library with the production version after testing is completed
  - Allow read-only access to source code
  - Require that program naming conventions have a unique identifier to distinguish test from production versions
  - Implement screening controls of job control language to prevent production execution of a test program caused by the use of wrong program name
**PROJECT MANAGEMENT**

- **Critical Path Methodology (CPM):** A critical path is the one whose sum of activity is longer than that for any other path through the network. The path is important because, if everything goes according to schedule, its length gives the shortest possible completion time of the overall project.

  ![PERT Chart](chart.png)

- **PERT chart for a project with five milestones (10 through 50) and six activities (A through F).** The project has two critical paths: activities B and C, or A, D, and F – giving a minimum project time of 7 months.

**PROJECT MANAGEMENT**

- **Program Evaluation and Review Technique (PERT):** Assumes that a project is a collection of activities or tasks. The activities can be started and stopped independent of each other or have precedent relationships. Precedent relationships preclude the start of certain activities until others are complete (e.g. surfacing a road must be preceded by the laying of the roadbed).

  - Advantages of PERT
    - Greatly improved control over complex development work & production programs
    - Capacity to distill large amounts of data in brief, orderly fashion
    - Requires a great deal of planning to create a valid network
    - Represents the advent of the management-by-exception principle
    - People in different locations can relate their efforts to the total task requirements of a large program
    - Downstream savings are achieved by earlier and more positive action by part of the management in the early stages of the project
PROJECT MANAGEMENT

- Limitations of PERT
  - Little interconnection between different activities pursued
  - Requires constant upgrading and reanalysis of schedules and activities
  - Requires greater amount of detail work
  - Does not contain the quantity information, only time information is available

- Applications of PERT & CPM
  - Construction & maintenance of plants, highways, dams etc.
  - Planning of retooling programs for high volume products in plants such as automotive and appliance plants
  - Introduction of a new product
  - Installation of a computer system
  - Acquisition of a company

PERT VS CPM

- PERT and CPM are very similar in their approach; however two distinctions are usually made between them.
- The first distinction relates to the way in which activity duration are estimated:
  - In PERT, three estimates are used to form a weighted average of the expected completion time of each activity, based on a probability distribution of completion times. Thus, PERT is considered a probabilistic tool.
  - In CPM, there is only one estimate of duration; that is, CPM is a deterministic tool.
- The second distinction is that CPM allows an explicit estimate of costs in addition to time.
- Thus, while PERT is basically a tool for planning and control of time, CPM can be used to control both the time and the cost of the project.
**PROJECT MANAGEMENT**

- A Gantt chart is a type of bar chart, developed by Henry Gantt, that illustrates a project schedule. Gantt charts illustrate the start and finish dates of the terminal elements and summary elements of a project. Terminal elements and summary elements comprise the work breakdown structure of the project. Some Gantt charts also show the dependency (i.e., precedence network) relationships between activities. Gantt charts can be used to show current schedule status using percent-complete shadings and a vertical "TODAY" line as shown here.

![Gantt Chart Example]

**PROJECT MANAGEMENT**

- A work breakdown structure (WBS), in project management and systems engineering, is a deliverable oriented decomposition of a project into smaller components. It defines and groups a project's discrete work elements in a way that helps organize and define the total work scope of the project.

- Time Box Management: In time management, a time box allot a fixed period of time for an activity. Timeboxing plans activity by allocating time boxes; and is a distinctive feature of several unorthodox project management approaches.
SYSTEM DEVELOPMENT TOOLS
- Computer-aided software engineering (CASE) is the scientific application of a set of tools and methods to a software system which is meant to result in high-quality, defect-free, and maintainable software products. It also refers to methods for the development of information systems together with automated tools that can be used in the software development process.

- Upper Case: used to describe and document business and application requirements
- Middle Case: used for developing the detailed designs
- Lower Case: deal with the generation of program code and database definitions

The IS Auditor needs to consider the following with CASE tools:
- CASE tools help in design process, but do not ensure the design, programs and system are correct or fully meet the needs of the organization
- CASE tools should compliment and fit into the app development methodology
- The integrity of data moved between various tools needs to be monitored
- Changes to apps should be reflected in stored CASE product data
- App controls need to be designed
- The CASE repository needs to be secured on a need to know basis
- Strict version control should be maintained on this database

4th Generation Languages (4GL)
- Portability
- Software facilities
- Workbench
- Simple language subsets
AUDITING INFRASTRUCTURE & OPERATIONS

HARDWARE

- Invitation to Tender/ Request For Proposal or specification should include the following:
  - Organizational description indicating whether the computer facilities are centralized or decentralized
  - Information processing requirements such as:
    - Major existing application systems and future application systems
    - Workloads and performance requirements
    - Processing approaches to be used (for example, online/batch, client server, real-time databases, continuous operation)
  - Hardware requirements such as:
    - CPU processing speed
    - Peripheral devices
    - Data preparation/input devices that convert and accept data for machine processing
    - Direct entry devices (terminals, point-of-sale terminals or automatic teller machines)
    - Networking capability (such as Ethernet connections, modems and ISDN connections)
  - System software requirements such as:
    - Operating system software (current version and any upgrades required)
    - Compilers
    - Program library packages
    - Database management packages and programs
    - Communications software
    - Security/access control software

by: Bilal Mahmood Sulehri
HARDWARE

- Invitation to Tender/ Request For Proposal or specification should include the following: (continued..)
  - Support requirements such as:
    - System Maintenance
    - Training
    - Backup
  - Adaptability requirements such as:
    - Hardware/software upgrade capabilities
    - Compatibility with existing hardware/software platforms and Changeover to other equipment capabilities
  - Constraints such as:
    - Staffing levels
    - Existing hardware capacity
    - Delivery dates
  - Conversion requirements such as:
    - Test time for the hardware/software
    - System conversion facilities
    - Cost/pricing schedule

by: Bilal Mahmood Sulehri

HARDWARE/ SOFTWARE ACQUISITION

- When purchasing (acquiring) hardware/software from a vendor, consideration should be given to the following:
  - Testimonials/visits to other users
  - Provision for competitive bidding
  - Analysis of bids against requirements
  - Comparison of bids against each other
  - Analysis of vendor financial condition
  - Analysis of the vendor’s capability to provide maintenance and support (including training)
  - Review of delivery schedules against requirements
  - Analysis of hardware/software upgrade capability
  - Analysis of security and control facilities
  - Evaluation of performance against requirements
  - Review and negotiation of price
  - Review of contract terms (including right to audit clauses)
  - Preparation of a formal written report summarizing the analysis for each of the alternatives and justification for the selection based on benefits and cost

by: Bilal Mahmood Sulehri
HARDWARE/SOFTWARE ACQUISITION

- The following criteria should be considered during Evaluating Vendor Proposals
  - Turnaround time
  - Response time
  - System reaction time — how the operating system processes information
  - Throughput
  - Workload
  - Compatibility
  - Capacity
  - Utilization

- Information typically maintained by Hardware Maintenance Program includes
  - Reputable service company information for each IS hardware resource requiring routine maintenance
  - The maintenance schedule
  - Maintenance cost
  - The maintenance performance history, both planned and exceptional

REPORTS TO MONITOR HARDWARE

- **Hardware Error Reports** — These reports identify CPU, Input/Output (I/O), power and storage failures. These reports should be reviewed by IS operations management to ensure that equipment is functioning properly, to detect failures and initiate corrective action.

- **Availability Reports** — These reports indicate the time periods during which the computer is in operation and available for utilization by users or other processes. A key concern addressed by this report is excessive IS inactivity referred to as down time. This inactivity may indicate inadequate hardware facilities, excessive operating system maintenance, lack of preventive maintenance, inadequate physical plant (for example, power supply or air conditioning) or inadequate training for operators.

- **Utilization Reports** — document the use of the machine and peripherals. Software monitors are used to capture utilization measurements for processors, channels and secondary storage media such as disk and tape drives. Depending on the operating system, resource utilization for multi-user computing environments found in mainframe/large-scale computers should average in the 85 percent to 95 percent range, with allowances for utilization that occasionally reach 100 percent and may at times dip below 70 percent. Trends provided by utilization reports can be used by IS management to predict where more or fewer, processing resources are required.
HARDWARE

- If utilization is routinely above the 95 percent level, IS management may consider reviewing user and application patterns to free up space, upgrading computer hardware and/or investigating where "savings can be made by eliminating non-essential processing or moving less critical processing to less demanding periods (such as during the night). If the utilization is routinely below the 85 percent level, there is a need to determine whether hardware exceeds processing requirements.

- Capacity Management: Monitoring of the computer resources to ensure that the available resources are being used efficiently and effectively. Following information is needed for capacity planning:
  - CPU utilization
  - Computer storage utilization
  - Telecommunications and WAN bandwidth utilization
  - Terminal utilization
  - I/O channel utilization
  - Number of users
  - New technologies
  - New applications
  - Service level agreements

by: Bilal Mahmood Sulehri

HARDWARE

- The goals of computer capacity management are:
  - Ensure that applications systems are properly designed and configured to give efficient performance
  - Have sufficient computer capacity for present and future operations
  - Contain the cost of computing

- Hardware Acquisition Review is performed to determine:
  - Whether hardware acquisition plan is compared regularly to business plan
  - Whether environment is adequate to accommodate currently installed and proposed hardware
  - Whether acquisition plan is in line with the IS plans
  - Whether hardware acquisition plan has taken into consideration technological obsolescence of both the installed equipment and the proposed equipment
  - The adequacy of documentation for hardware and software specs.

by: Bilal Mahmood Sulehri
DATABASE MODELS

- Hierarchical Database Model — This model allows the data to be structured in a parent/child/relationship (each parent may have many children, but each child would be restricted to having only one parent). Under this model, it is difficult to express relationships when children need to relate to more than one parent. When the data relationships are hierarchical, the database is easy to implement, modify and search. However, this also can lead to data redundancy.

- Network Database Model — This model allows children to relate to more than one parent. A disadvantage to the network model is that such structures can be extremely complex and difficult to comprehend, modify or reconstruct in case of failure.

- Relational Database Model — This model, is independent from the physical implementation of the data structure. The relational database organization has many advantages over the hierarchical and network database models.

Advantages of Relational Model

- Easier for users to understand and implement in a physical database system
- Easier to convert from other database structures
- Projection and joint operations (referencing groups of related data elements not stored together) are easier to implement
- Access control over sensitive data is easy to implement
- Faster in data search
- Easier to modify than hierarchical or network structures
DATABASE CONTROL

- It is critical that database integrity and availability be maintained.
- Establish definition standards and closely monitor for compliance.
- Establish and implement data back up and recovery producers to ensure database availability.
- Establish various levels of access controls for data items, tables and files to prevent inadvertent or unauthorized access.
- Establish controls to handle concurrent access problems, such as, multiple users desiring to update the same data elements at the same time.
- Establish controls to ensure accuracy, completeness and consistency.
- Use database checkpoints to restart processing after a system failure at points in the job stream that minimize data loss and recovery efforts.
- Perform database restructuring procedures when making logical, physical and procedural changes.
- Use database performance monitoring tools to monitor and maintain database efficiency.
- Minimize the ability to sue non-system means, for instance, those outside security control, to access the database.

DATABASE CONTROL

Program Library Management Systems
- Integrity
- Update
- Reporting
- Interface

Utility programs
- Required normal processing operational
- Five functional areas
  - To understand application systems
  - To facilitate assessing or testing data quality
  - To test a program’s ability to function correctly and maintain data integrity
  - To assist in faster program development
  - To improve operational efficiency

by: Bilal Mahmood Sulehri
DATABASE CONTROL

System software Acquisition
- Business, functional and technical needs and specification
- Cost/benefits(s)
- Obsolescence
- Compatibility with existing systems
- Security
- Demands on existing staff
- Training and hiring requirements
- Future growth needs
- Impact on system performance and the network.
- Software development project manager to oversee the project development process.
- Software system engineers to provide system requirements
- Following individuals may be involved in supporting roles.
- Business sector and application specialists
- Database and capacity planning specialists
- Data administrator
- Network and technical support specialists.
- Vendor personnel
- Quality assurance personnel to ensure the development and delivery of a contractually acceptance product.
- Subject matter experts to provide assistance in defining operations requirements
- IS management to ensure the software will be consistent with the goals and objectives established for the organization.

by: Bilal Mahmood Sulehri

Software Alternatives

Software alternative analysis should include an evaluation of the following
- Criteria
- Cost factors to be development versus purchase
- Software cost
- Initial and continuing support availability
- Delivery schedule
- Requirements and constraints to use
- Capabilities and limitations of the software.
- Potential risk of using future costs.
- Alternative approaches
- Selection advice from vendors, comparable installations and consultants.
- Compatibility with existing in house system software operating systems, database managements systems and communications software
- Financial stability of software suppliers
- Technical expertise of software suppliers.

by: Bilal Mahmood Sulehri
SOFTWARE ACQUISITION

Cost/Benefit Analysis
- Current system operating cost
- Resources and facilities
- Current systems capabilities and limitations
- Proposed software capabilities and benefits
- Resources and facilities required to maintain the proposed system
- Ability for future system enhancement
- Opportunity to provide greater efficiency or cost effective use of processing resources
- Appropriateness

System software implementation and change control procedures
- Program testing to check the logic of individual programs
- System testing to ensure program and file consistency as they are linked together and that they meet system requirements.
- Parallel testing of the new software simultaneously with the existing software.

Software licensing issues
- To prevent or detect software licensing violations, the IS Auditor should:
  - Review documented policies and procedures guarding against unauthorized usage or copying of software.
  - Review the listing of all standard application software used and licensed.

DATABASE CONTROL

Procedures to prevent software license violations include:
- Centralizing control and automated distribution and the installation of software
- Requiring that all PCs be diskless workstations and have the workstations access applications from a secured LAN.
- Installing metering software on the LAN and require all PCs to access applications through the metered software.
- Regularly scanning user PCs either form the LAN or directly to ensure that no unauthorized copies of software have been loaded on the PC.

System software review
- Interview technical service, other personnel regarding
- Review system software selection procedures
- Review the feasibility study and selection process
- Review controls over the installation of changed system
- Review system software maintenance activities
- Review system software change controls to determine
- Review systems documentation specifically
- Review and test systems software implementation
- Review authorization documentation is performed
- Review system software security
- Review database supported information systems controls

by: Bilal Mahmood Sulehri
DATABASE CONTROL

Computer Operations
- Running jobs/macros/programs
- Restarting computer applications after an abnormal termination has been investigation and resolved by the responsible department.
- Facilitating timely backup of computer files.
- Observing the information processing facility for unauthorized entry
- Monitoring adherence to documented job schedules as established by IS and business management
- Participating in tests of disaster recovery plans

Procedures
- Operator procedures based on computer and peripheral equipment operating instructions and job flows
- Procedures for rectifying machine or program failures and escalation of unresolved failures
- Instructions for output report distribution
- Procedures for obtaining files from the off-line library and returning files to the library
- Procedures for reporting run delays
- Procedures for reporting and correcting equipment failures and job processing delays.

by: Bilal Mahmood Sulehri
DATABASE CONTROL

Input/Output Control Function

- Input is processed accurately and in a timely manner.
- Output is produced in the proper format and is distributed to the appropriate people. With the availability of communication facilities, the high-speed printing of paper documents (i.e. reports, bills, etc.) is often accomplished at a remote and sometimes separate location from the IS department.
- Output that becomes input to the next system in sequence is accurate and complete and produced in a timely manner.
- Correct files were used during processing
- Proper actions are taken by operators.
- No evidence exists which indicates that data was altered in an unauthorized manner.

Data entry personnel

- Key verification - while many types of verification techniques may be employed during the data entry process, one-to-one verification, though often impractical for verifying large amounts of data entry, will yield the highest degree of confidence that entered is error free.
- Segregation of data entry functions from data entry verification
- Maintaining a log/record detailing the time, date, employee's initials/user-ID and progress of various data preparation and verification tasks.

by: Bilal Mahmood Sulehri

DATABASE CONTROL

Management of IS Operations

- Resources Allocation: IS management is responsible for ensuring that the necessary resources are available to perform the planned activities within the IS function.
- Standards and Procedures: IS management is responsible for establishing the necessary standards and procedures (or all operations in accordance with the overall business strategies and policies.

Control Functions

- Ensuring that detailed schedules exist for each operating shift
- Planning to ensure the most efficient and effective use of an operation's resources.
- Authorizing changes to operations schedules
- Reviewing console log activities
- Ensuring information systems processing can recover in a timely manner form both minor and major disruptions of operations.
- Monitoring system performance and resources usage to optimize computer resource utilization
- Anticipating equipment replacement/capacity to maximize current job throughout and to strategically plan future acquisitions.
- Monitoring the environment and security of the facility to maintain proper conditions for equipment performance
- Ensuring changes to hardware and software do not cause undue disruption to normal processing
- Maintaining job accounting reports and other audit records.
- Limiting physical access to computer resources to those who require it.

by: Bilal Mahmood Sulehri
DATABASE CONTROL

Abnormal job termination Reports.
• Poor application design, development or testing. Inadequate operation instructions
• Inadequate operations support
• Inadequate operator training or performance monitoring.

Console Log
• Only approved programs access sensitive's data.
• Utilities or service aids that can alter data files and program libraries are used only for authorized purposes.
• Approved programs are run only when scheduled and conversely, unauthorized runs do not take place.
• The correct data file generation is accessed for production papoose.
• Data files reported to be password-protected are protected.

Database Control

Support /Help Desk

Support functions include:
• Determining the source of computer problems and taking appropriate corrective actions
• Initiating problem reports as required and ensuring that problems are resolved in a timely manner
• Obtaining detailed knowledge of the operating system and other systems software
• Answering inquiries regarding specific systems
• Controlling the installation of vendor and system software to improve its efficiency and to customize the system based on organizational requirements and computer congregation
• Providing technical support for computerized telecommunication processing
• Maintaining documentation of vendor software including issuance of new releases and problem fixes, as well as documentation of in-house developed systems and utilities.

The basic function of the help desk is to perform the following:
• Document problems that arise form users and initiate problem resolution
• Escalate the issue according to priority
• Follow up on unresolved problems
• Close out resolved problems noting proper authoritarian to close out the problem by the user
DATABASE CONTROL

Computer operations
Restricting operator access capabilities
• Operators responsibilities should be limited to running of the computer and related peripheral equipment.
• Operators should have restricted form correcting program and data problems.
• Operators should have restricted access to utilities that allow system fixes to software and or data.
• Operators should have limited access to production source code and data libraries, including run procedures.

Scheduling:
• Operations should record jobs that are to be processed and their required data files.
• Operations should schedule jobs for processing on a predetermined basis and perform them using either automated scheduling software of a manual schedule.
• Using exception-processing procedures to obtain written or electronic approval form application owners to run jobs or programs in another sequence.
• Operators should obtain written or electronic approval form owners when scheduling on request only jobs.
• Operators should record all exception-processing request log to determine the appropriateness of procedures performed.

by: Bilal Mahmood Sulehri

DATABASE CONTROL

Executing re-run handling:
• All re-execution of jobs should be properly authorized and logged for IS management review.
• Procedures should be established for re-running jobs to ensure the correct input files are used and that subsequent jobs in the sequence are also re-am if appropriate.
• Librarian Access Capabilities.
• Librarian should not have computer hardware access.
• Librarian should only have access to the tape management system.
• Access to library facilities should be restricted to authorized staff.
• Removal of files should be restricted by production scheduling software.
• Librarian should handle the receipt and return of foreign media entering library.
• Logs of the sign-in and sign-out of data files and media should be maintained.
• Contents and location of off-line storage
• Off-line file storage media containing production system programs and data should be clearly marked as to content.
• Off-line library facilities should be located away from the computer room. Audit procedures should include a review of policies and procedures for:
• Administering the off-line library
• Checking out/in tape media including signature authorizations.
• Identifying labeling, delivering and retrieving off-site backup files.
• Inventorying the system for on-site and off-site tapes including specific storage locations of each tape.
• Scratching, deleting and securing disposal/destruction of tape datasets including signature authorization.

by: Bilal Mahmood Sulehri
DATABASE CONTROL

Data Entry Control
- Authorization of input documents
- Reconciliation of batch totals
- Segregation of duties between the person who keys the data and the person who reviews the keyed data for accuracy and errors.

Audit procedures for data entry should include a review of the controls and the procedures to determine whether:
- Adequate controls exist.
- IS personnel are adhering to the established policies.
- Proper segregation of duties is being maintained.
- Control reports are being produced, maintained and reviewed. The control reports are accurate and complete.
- Authorization forms are complete and contain appropriate signatures.

DATABASE CONTROL

These concerns include the following:
- Remote access to master console is often granted to stand-by operators for contingency purposes such as failure in the automated software. Therefore communication access is opened to allow for very risky, high powered, console commands. Communication access security must be extensive. This would include using leased lines and dial-back capabilities.
- Contingency plans must allow for the proper identification of a disaster in the unattended facility. In addition, the automated operation software of manual contingency produces must be adequately documented and tested at the recovery site.
- Because vital IS operations are performed by systems, poorer program change controls and access controls need to be applied to this software, also, testing of the software should be performed on a periodic basis especially when changes or updated are applied.
- Ensure that errors are not hidden by the software and that all errors in operator notification.

Auditing databases
- Design
- Verify
- Review the logical schema
- The physical scheme
- Access
- Administration
- Interfaces
- Portability
DISASTER RECOVERY AND BUSINESS CONTINUITY PLANNING

DISASTER RECOVERY PLANNING

- Business impact analysis: Involves identifying the various events that could negatively affect the continuity of operations and their impact on organization.

- Critical recovery time period: is the window of time in which the business processing must be resumed before suffering significant or unrecoverable loss.

- Phases of Business Continuity Planning:
  - Business impact analysis (BIA)
  - Developing business recovery strategies
  - Develop detailed plan
  - Implement plan
  - Test an implemented plan

- Three important questions:
  - What are critical information resources related to organization's critical business processes? (is it your server, hardware or software)
  - What is the critical recovery time/period for information resources?
  - What is the system risk ranking (some are very risky or low risky)

by: Bilal Mahmood Sulehri
DISASTER RECOVERY PLANNING

- System risk ranking:
  - Critical system [Need to be replaced by identical capabilities]
  - Vital systems [Can be performed manually for a brief period of time at high cost]
  - Sensitive system [Can be performed manually for extended time period at tolerable cost]
  - Non critical system [Can be performed manually for extended time period at litter or no extra cost.]

- Factors to be accounted for while developing business recovery strategies.
  - Criticality of business processes
  - Cost
  - Time required to recover
  - Security

by: Bilal Mahmood Sulehri

DISASTER RECOVERY PLANNING

- Types of strategies /recovery alternatives
  - Reciprocal agreement with other companies: Agreement with two or more organizations with similar equipment or applications (it is inexpensive but difficult to reinforce)
  - Duplicate information processing facilities (IPF): Dedicated self developed recovery sites that can backup critical applications.
  - Hot sites: Fully configured and ready to operate within several hours. Installed with low power processor to take care of critical applications. Additional needs are staff, programs, data files and documentation
  - Warm sites: Partially configured usually with network connections and selected peripheral equipments such taps and disk drives.
  - Cold sites: Equipped with basic facilities only like electrical wiring, air conditioning and flooring.
DISASTER RECOVERY PLANNING

- Several principles must be in place to ensure the viability of duplicate IPF:
  - The site chosen must not be subject to the same natural disasters
  - There must be a coordination of hardware and software strategies
  - Resource availability must be ensured. Workload of the sites must be monitored
  - Regular testing is necessary

- Advantages of reciprocal agreements
  - Low cost
  - May be the only option available due to shortage of hot sites or unique equipment

- Disadvantages of reciprocal agreements
  - Usually not enforceable
  - Differences in equipment configuration
  - Un-notified changes in workload or equipment configurations

Critical questions to cover in a reciprocal agreement:
- How much time will be available at the host computer site?
- What facilities and equipment will be available?
- Will staff assistance be provided?
- How quickly can access be gained to the host recovery facility?
- Can data and voice communication links be established at the host site?
- How long can emergency operation continue?
- How frequently can the system be tested for compatibility?
- How will confidentiality of data be maintained?
- What type of security will be afforded for IS operations and data?
- Are there certain times of the year when partner’s facilities are not available?

by: Bilal Mahmood Sulehri
DISASTER RECOVERY PLANNING

- Contractual provisions for the use of third party (hot, cold, warm) sites should cover the following:
  - Configuration
  - Disaster
  - Speed of availability
  - Subscribers per site
  - Subscribers per area
  - Preference
  - Insurance
  - Usage period
  - Communications
  - Warranties
  - Audit
  - Testing
  - Reliability

- Procuring hardware: vendor or third party. (second hand market)

by: Bilal Mahmood Sulehri

ORGANIZATION AND ASSESSMENT OF RESPONSIBILITIES

1. Emergency action team (first team who does evacuation)
2. Damage assessment team (assesses damage and estimates time for recovery)
3. Emergency management team (coordinates the activities of all other teams)
4. Emergency Operation team (manages system operations at recovery site)
5. Transportation team (locates a recovery site if not determined and coordinates the transportation of employees to disaster recovery sites)
6. Network recovery team (re-routes wide area voice and data communication traffic)
7. Communication team (establishes a user/system network solicits and installs communication hardware)
8. User hardware team (coordinates the delivery and installation of user terminals, printers, typewriters, photocopiers and other equipment)
9. Software team (restores system packs, loads and tests operating system)
10. Application team (restores user packs and application programs on the backup system)
11. Security team (monitors the security of system and communication links)
12. Off site storage team (obtains packages and shifts media and records to the recovery facilities)
13. Data preparation and records team (updates the application database)
14. Administrative support team (serves as a message centre for the user recovery site)
15. Supplies team (coordinates supply of necessary office and computer supplies)
16. Salvage team (manages the relocation project)
17. Relocation team (coordinates the process of moving from the backup site to a new location or to the restored original location)

by: Bilal Mahmood Sulehri
**BUSINESS CONTINUITY PLAN**

- Following should be agreed upon for planning, implementation and evaluation of BCP:
  - Goals/requirements for each phase
  - Alternate facilities to perform tasks and operations
  - Critical information resources
  - People/individuals responsible for completion
  - Scheduling of activities with priorities established

- Directory of key decision making personnel should contain the following information:
  - Prioritized list of contacts
  - Primary & emergency telephone numbers and addresses for each critical contact person
  - Phone numbers and addresses of representatives of equipment and software vendors
  - Phone numbers of contacts within the organization that have been assigned to provide supplies and equipment etc.
  - Phone numbers of contacts at recovery facilities
  - Phone numbers of critical person at off-site media storage facilities & the contact person of the company who is authorized to retrieve these
  - Phone numbers of insurance policy agents
  - Phone numbers of contacts at contract personnel services

**TESTING OF A PLAN**

- Phases of test execution:
  - Pre test: Set of action necessary to set the stage for the actual test.
  - Test: Real action of the business continuity test. Actual operational activities are executed to test the specific objectives of the business continuity test.
  - Post test: Clean up of group activities

- Types of test:
  - Paper test (paper walkthrough of the plan)
  - Preparedness test (localize version of a full test)
  - Full operational test (it is one step away from an actual service disruption)

- Analyze results of the tests performed:
  - Time (elapse time for completion of prescribed test.)
  - Amount of work performed at backup site
  - Count no. of vital record successfully carried to the backup sites and no. of critical systems successfully recovered.
  - Accuracy of data entry at the recovery site.

- Plan maintenance:
  - Changes in the business strategy
  - New application
  - Changes in the IT infra structures
  - As per environment
  - Any mishap

by: Bilal Mahmood Sulehri