Revision in Study Material in December 2011

CHAPTER 2: SYSTEM DEVELOPMENT LIFE CYCLE METHODOLOGY

2.3.6 Agile Methodologies *(Old para 2.3.6 is replaced as follows)*

(a) This is a group of software development methodologies based on the *iterative and incremental* development, where requirements and solutions evolve through collaboration between self-organizing, cross-functional teams.

(b) It promotes adaptive planning, evolutionary development and delivery; time boxed iterative approach and encourages rapid and flexible response to change.

(c) It is a conceptual framework that promotes foreseen interactions throughout the development life cycle.

Basic Principles

Following are the key principles of this methodology:

(i) Customer satisfaction by rapid delivery of useful software;

(ii) Welcome changing requirements, even late in development;

(iii) Working software is delivered frequently (weeks rather than months);

(iv) Working software is the principal measure of progress;

(v) Sustainable development, able to maintain a constant pace;

(vi) Close, daily co-operation between business people and developers;

(vii) Face-to-face conversation is the best form of communication (co-location);

(viii) Projects are built around motivated individuals, who should be trusted;

(ix) Continuous attention to technical excellence and good design;

(x) Simplicity;

(xi) Self-organizing teams; and

(xii) Regular adaptation to changing circumstances.

Strengths

(i) Agile methodology has the concept of an adaptive team, which is able to respond to the changing requirements.

(ii) The team does not have to invest time and effort and finally find that by the time they delivered the product, the requirement of the customer has changed.

(iii) Face to face communication and continuous inputs from customer representative leaves no space for guesswork.

(iv) The documentation is crisp and to the point to save time.

(v) The end result is the high quality software in least possible time duration and satisfied customer.

Weaknesses

(i) In case of some software deliverables, especially the large ones, it is difficult to assess the efforts required at the beginning of the software development life cycle.

(ii) There is lack of emphasis on necessary designing and documentation.

(iii) Agile increases potential threats to business continuity and knowledge transfer. By nature, Agile projects are extremely light on documentation because the team focuses on verbal communication with the customer rather than on documents or manuals.

(iv) Agile requires more re-work. Because of the lack of long-term planning and the lightweight approach to architecture, re-work is often required on Agile projects when the various components of the software are combined and forced to interact.

(v) The project can easily get taken off track if the customer representative is not clear about the final outcome that they want.

(vi) Only senior programmers are capable of taking the kind of decisions required during the development process. Hence, it has no place for newly appointed programmers, unless combined with experienced resources.

(vii) Agile lacks the attention to outside integration. Because Agile teams often do not invest the time in identifying and designing the integration points with other systems in advance, the need for an integration point can become a last-minute surprise that often requires re-work, additional time, removal from scope, or a poor-quality product.

2.6.4 System Development Tools:

(a) Structured English: Elements, Keywords, Example 2.6.1 deleted.

(b) Flow Chart: Types, benefits and limitations of flowchart, Examples 2.6.2, 2.6.3 and 2.6.4 deleted.

(c) Decision Tree: Example 2.6.5 along-with Table 2.6.2 and figure 2.6.5 which are part of the example - deleted.

(d) **Decision Table:** Example 2.6.6 along-with Table 2.6.3 which is part of the example - deleted.

Example 2.6.7 along-with Table 2.6.4 which is part of the example - deleted.

2.14 Auditors' Role In SDLC *(Old para 2.14 Organisational Structure … is replaced as follows)*

The **audit of systems under development** can have three **main objectives**:

(a) to provide an opinion on the efficiency, effectiveness, and economy of project management;

(b) to assess the extent to which the system being developed provides for adequate audit trails and controls to ensure the integrity of data processed and stored; and

(c) to assess the controls being provided for the management of the system's operation.

- For the **first objective** to achieve, an auditor will have to attend project and steering committee meetings and examine project control documentation and conducting interviews. This is to ensure what project control standards are to be complied with, (such as a formal systems development process) and determining the extent to which compliance is being achieved.
- For addressing **second objective**, the auditor is can examine system documentation, such as functional specifications, to arrive at an opinion on controls. The auditor's opinion will be based on the degree to which the system satisfies the general control objectives that any Information Technology system should meet. A list of such objectives should be provided to the auditee.

- The same is true for the **third objective**, viz. system's operational controls. The auditor should provide the a list of the standard controls, over such operational concerns as response time, CPU usage, and random access space availability, that the auditor has used as assessment criteria.

An Auditor may adopt a **rating system** such as on scale of 1 to 10 in order to give rating to the various phases of SDLC. E.g. in rating a Feasibility Study, auditor can review Feasibility Study Report and different work products of this study phase.

An interview with personnel who have conducted this feasibility study can be conducted. Depending on the content and quality of the Feasibility Study report and interviews, an auditor can arrive at a rating between 1 to 10 (10 being best).

After deriving such a rating for all the phases, the auditor can form his/her overall opinion about the SDLC phases.

In order to **audit technical work products** (such as database design or physical design), auditor may opt to include a technical expert to seek his/her opinion on the technical aspects of SDLC.

However, auditor will have to give control objectives, directives and in general validate the opinion expressed by technical experts. Some of the control considerations for an auditor are:

- Documented policy and procedures;
- Established Project team with all infrastructure and facilities ;
- Developers/ IT managers are trained on the procedures ;
- Appropriate approvals are being taken at identified mile-stones;
- Development is carried over as per standards, functional specifications;
- Separate test environment for development/ test/ production / test plans;
- Design norms and naming conventions are as per standards and are adhered to;
- Business owners testing and approval before system going live;
- Version control on programs;
- Source Code is properly secured;
- Adequate audit trails are provided in system; and
- Appropriateness of methodologies selected.

Further, **Post-Implementation Review** is performed to determine whether the system adequately meets earlier identified business requirements and needs (in feasibility studies or Requirements Specifications).

Auditors should be able to determine if the expected benefits of the new system were realized and whether users are satisfied with the new system.

In post implementation review, auditors need to review which of the SDLC phases have not met desired objectives and whether any corrective actions were taken.

If there are differences between expectations and actual results, auditors need to determine the reasons for the same. E.g. it could be due to incomplete user requirements. Such reasons can help auditors to evaluate the current situation and offer guidelines for future projects.

Master Checklist

The **process objectives** are:

- To ensure an appropriate acquisition and / or development of information systems including software, and
- To maintain the information systems in an appropriate manner.

The following checklist may be used by the IS Auditors for this purpose:

Sr. No	Check Point	Statues
1.	Whether information system acquisition and / or development policy and procedure documented?	
2.	Whether system acquisition and / or development policy and procedure approved by the management?	
3.	Whether the policy and procedure cover the following: ♦ Problems faced in the existing system and need for replacement ♦ Functionality of new IS ♦ Security needs ♦ Regulatory compliance ♦ Acceptance Criteria ♦ Proposed roles and responsibilities ♦ Transition/ Migration to new IS ♦ Interfaces with legacy systems ♦ Post implementation review ♦ Maintenance arrangements.	
4.	Whether policy and procedure documents are communicated / available to the respective users?	
5.	Whether policy and procedure documents are reviewed and updated at regular intervals?	
6.	Whether the organization has evaluated requirement and functionalities of proposed IS? (Verify the requirement analysis conducted at three levels viz. process level, application level and organization level. Verify the site visit reports and other customer references obtained with respect to functionalities of proposed IS).	
7.	Whether the organization carried out feasibility study in respect of the following ♦ Financial feasibility ♦ Operational feasibility ♦ Technical feasibility	

Sr. No	Check Point	Statues
8.	Whether the selection of vendor and acquisition terms considers the following: ♦ Evaluation of alternative vendors ♦ Specification on service levels and deliverables ♦ Penalty for delays ♦ Escrow mechanism for Source codes ♦ Customization ♦ Upgrades ♦ Regulatory Compliance ♦ Support and maintenance	
9.	Whether the organization has identified and assigned roles in development activities to appropriate stakeholders? (Verify the assigned roles should be on "need to know" and "need to basis". and duties of developers and operators are segregated).	
10.	Whether the organization has a separate development, test and production environments?	
11.	Whether the IS developed plan is prepared and approved by the management? (Verify that IS development plan to include: ♦ Input data elements, ♦ Validations controls viz. Field/ Transactions/ File with appropriate error reporting ♦ Process workflow ♦ data classifications with security are in place, viz. Read only for users, Read/ Write for authorized persons ♦ Output).	
12.	Whether the testing of IS includes: ♦ Confirms the compliance to functional requirements ♦ Confirms the compatibility with IS infrastructure ♦ Identifies bugs and errors and addresses them by analyzing root causes Escalating functionality issues at appropriate levels.	
13.	Whether the adequate documentation for: ♦ Preserving test results for future reference ♦ Preparation of manuals like systems manual, installation manual, user manual ♦ Obtaining user sign off / acceptance	

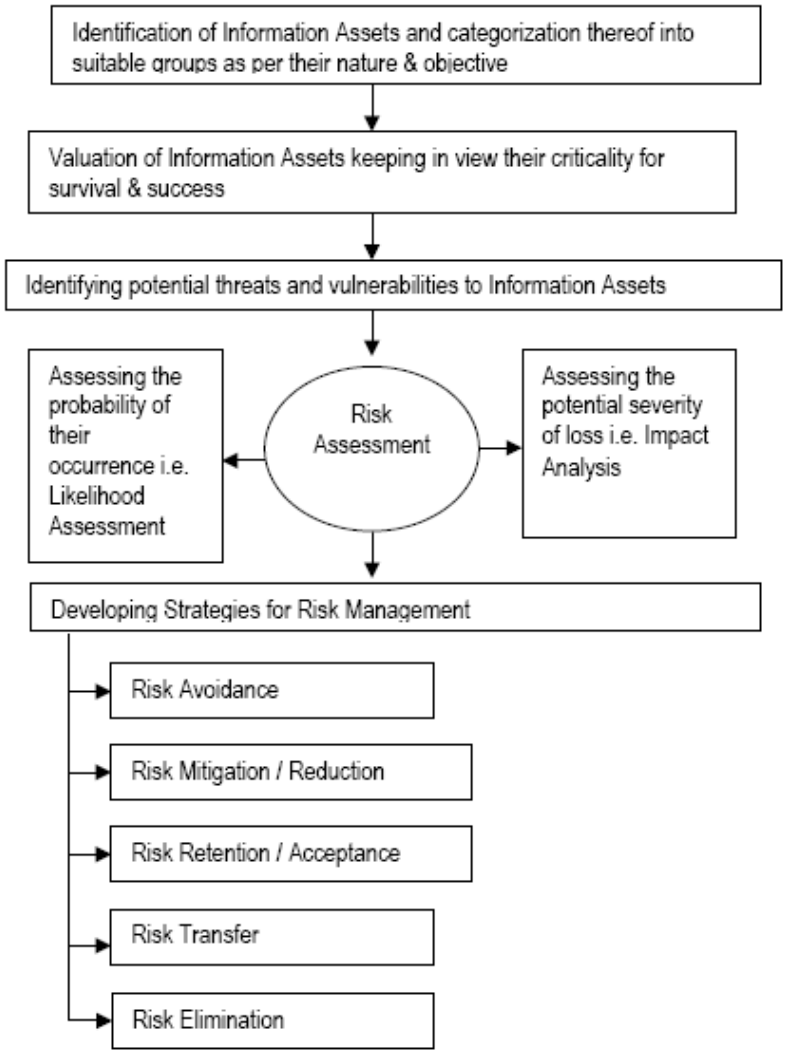
Sr. No	Check Point	Statues
14.	Whether the implementation covers the following? ♦ User Departments' involvement and their role ♦ User Training ♦ Acceptance Testing ♦ Role of Vendor and period of Support ♦ Required IS Infrastructure plan ♦ Risk involved and actions required to mitigate the risks ♦ Migration plan	
15.	If the development activities are outsourced, are the outsourcing activities evaluated based on the following practices: ♦ What is the objective behind Outsourcing? ♦ What are the in-house capabilities in performing the job? ♦ What is the economic viability? ♦ What are the in-house infrastructure deficiencies and the time factor involved? ♦ What are the Risks and security concerns? ♦ What are the outsourcing arrangement and fall back method? ♦ What are arrangements for obtaining the source code for the software? ♦ Reviewing the capability and quality of software development activities by visit to vendor's premises? ♦ Review of progress of IS development at periodic intervals.	
16.	Whether the organization carried out a post implementation review of new IS?	
17.	Whether a process exists for measuring vendors' performance against the agreed service levels?	
18.	Whether the post implementation review results are documented?	

5.6.1 Risk Management Process: *(Old para 5.6.1 is replaced as follows)*

The process of Information Risk Management typically involves the following steps:

- Identifying and classifying information assets,
- Valuation of the information and information assets as per their criticality
- Identifying threats and vulnerabilities to those assets,
- Measuring or assessing risk
- Developing strategies to manage risk

A pictorial representation of these steps is given as follows:



The detail of each step is given as follows:

Step 1: Identification of Information Assets

The first step in the information risk management process is to identify the information assets supporting critical business operations that need to be protected. The assets could fall under different groups which are:

- **Conceptual / Intangible Assets**
  - *Data and Information:* Business and related information contained in various storage devices such as hard disks or in transit may be subject to unauthorized disclosure, copying, theft, corruption or damage.
  - *Software:* It includes
    - Application software: application packages for accounting, payroll, sales etc. and
    - System software: operating system, utility programs, compiler, communication software, DBMS etc.

    Such programs may be susceptible to intentional or unintentional unauthorized modification by persons internal or external to the organization or by faulty technology processes.
- **Physical / Tangible Assets**
  - *People*: e.g. skilled users, analysts, programmers etc.
  - Hardware: e.g. mainframes, minicomputers, microcomputers, storage media, printers
  - Networking devices: e.g. communication lines, concentrators, hubs and switches etc.
  - Facilities: The computing and communication equipments such as servers could require special environment such as air-conditioned, dust free, humidity controlled facilities.
  - Documentation: e.g. printed forms, manuals, system and database documentation, IS policies & procedures

Step 2: Valuation of Information Assets

Data Valuation

(a) The information classification process focuses on business risk and data valuation. Not all data has the same value to an organization.

(b) Some data is more valuable to the people who are making strategic decisions because it aids them in making long-range or short-range business direction decisions.

(c) Some data, such as trade secrets, formulas, and new product information, are so valuable that its loss could create a significant problem for the enterprise in the marketplace by creating public embarrassment or by causing a lack of credibility.

Data Classification

(a) Information systems resources may require classifying or categorizing according to their sensitivity.

(b) This would depend upon the risks affecting such resources and impact resulting from exposure.

(c) Such classification is made for administrative convenience of implementing and maintaining access control systems and importantly optimizing the cost of security.

(d) Some information is more critical to a business than others such as production process information, formulas, strategic plans, research information.

(e) In the financial services industry, for example, information assets are very close to being financial assets. The loss of such information can jeopardize the existence of the business or create loss of goodwill and trust among stakeholders and loss of brand equity

(f) Compared to this, the organization may also have information, which is of less consequence in the event of their loss, such as a list of customers, details of employees' salaries, etc.

(g) Thus in order to ensure cost-effective controls, it is beneficial to classify the entire organizational information.

(h) This also enables fine tuning of access control mechanisms and avoids the cost of over-protecting and under protecting information.

The assets so identified and grouped may be categorized into different classes, which are:

- **Top secret:** This indicates the highest classification wherein the compromise of the confidentiality, integrity and availability can endanger the existence of the organization. Access to such information may be restricted to either a few named individuals in the organization or to a set of identified individuals.
- **Secret:** Information in this category is strategic to the survival of the organization. Unauthorized disclosure could cause severe damage to the organization and stakeholders.
- **Confidential:** Information in this category also needs high levels of protection but unauthorized disclosure may cause significant loss or damage. Such information is highly sensitive and should be well protected.
- **Sensitive:** Such information requires higher classification as compared to unclassified information. Disclosure may cause serious impact.
- **Unclassified:** Information that does not fall in any of the above categories finds place here. This also implies that the nature of the information is such that its unauthorized disclosure would not cause any adverse impact on the organization. Such information may also be made freely available to the public.

Another type of classification, popular in commercial organizations, can be: Public, Sensitive, Private and Confidential.

Step 3: Identifying the potential threats

Threat can be defined as an event that contributes to the interruption or destruction of any service, product or process. Common *classes of threats* are:

- Errors
- Malicious damage/attack
- Fraud
- Theft
- Equipment/software failure

Threats occur because of **vulnerabilities** associated with use of information resources. Vulnerabilities are characteristics of information resources that can be exploited by a threat to cause harm. *Examples of vulnerabilities* are:

- Lack of user knowledge
- Lack of security functionality
- Poor choice of passwords
- Untested technology
- Transmission over unprotected communication medium

Computer systems are vulnerable to threats that cause damage ranging from the loss of database integrity to the destruction of entire computer facilities. The sources of loss could be manifold from mere technological glitches to hackers, disgruntled or adventurous employees, data entry clerks, etc.

These threats could affect the **confidentiality, integrity or availability (CIA)** of system information or resources.

(a) **Confidentiality :** Confidentiality involves the protection of the organization's sensitive information from disclosure to unauthorized persons and processes.

Confidentiality threats in an IT environment include intentional as well as unintentional access to sensitive information. A few examples of exposures are given hereunder:

- *Improper application controls* in application software may lead to sensitive information being accessed by employees not having any need to access such information e.g. a payroll clerk may get accidental access to confidential records of management employees.
- *Unauthorized disclosure* arising from the access of confidential data on a system/network by inadvertent broadcast of data across the network, improper disposal of data etc.
- *Accidental access* to spool files used by printers may compromise sensitive information which may otherwise be protected by stringent access controls.

(b) **Integrity:** Integrity requires that the business information and related processes should not suffer any intentional or accidental unauthorized modification, which may result in serious consequences to the business.

Integrity violations in an IT environment are also common due to system errors which include: (i) corruption of files, (ii) power failures leading to unauthorized alteration in the values being transmitted or stored, (iii) erroneous program codes leading to alteration of values in data files etc.

Hence there is need to prevent the processes from performing any integrity violations.

A few examples of threats are given hereunder:

- A bank employee not having authority to credit files may tamper with the sanctioned amount of credit facilities by bypassing the application controls and making direct changes to data files or by gaining unauthorized access to the manager's login.
- Computer virus may cause corruption of data/program thereby causing loss of transactions or state of integrity of such transactions.
- Integrity violations in mission critical systems could cause irreparable damage to the business, threats to national security or loss of lives e.g. (i) corruption of tariff data files of Indian Railways, (ii) changes in values or parameter files of missile control systems, meteorological warning systems, (iii) corruption of program codes of autopilot systems used in flight control etc.

(c) **Availability:** Availability relates to whether the information and information technology processes are available to the authorized business users when required.

Availability therefore requires safeguarding the information systems and processes that are essential for supporting business processes, so as to ensure that the information systems and processes critical for conduct of business will be available to authorized users as and when required.

A few examples of exposures are given hereunder:

- The most common problems of availability occur due to improper capacity availability such as strangulated bandwidth, low computer resources as against the actual requirements such as processing capacity, storage capacity, number of terminals etc.
- Failure or improper functioning of power systems can lead to the computer systems being dysfunctional and hence not available for service e.g. power failure during banking hours.
- Intentional unavailability can also be created by hackers by launching denial-of-service attacks.

A clear idea of threats in the working environment will enable systems managers to implement the most cost-effective security measures.

Sources and Causes of Threats: Various threats can be grouped into environmental and man-made threats. Man made threats can again be categorized into internal and external threats.

Step 4: Information Risk Assessment :

Once the assets and corresponding potential threats have been identified, the systems are reviewed for weaknesses that can be exploited and the likelihood of those being exploited.

Information security professional or IS auditor here audits various systems and processes to find out vulnerabilities or weaknesses that can lead to a threat being materialized.

(a) **Vulnerability Assessment:**

- Vulnerability is a condition or weakness in (or the absence of) the safeguards, procedures, technical controls, physical controls or other controls that could be exploited by the threat.
- Sometimes the threat viewed in isolation may be misleading unless the vulnerabilities are taken into consideration.
- In most cases the threats attempt to exploit the vulnerabilities to cause loss or harm to the assets. For example, a hacker would look for loopholes in the architecture of the firewall to compromise the controls and gain unauthorized access to the networks.

(b) **Probability or Likelihood Assessment :**

- **Likelihood** is the estimation of the frequency, or the chance of a threat happening.
- A likelihood assessment considers the presence, tenacity and strength of threats, as well as, the effectiveness of safeguards.
- In general, historical information about many threats is weak, particularly with regard to human threats; hence the judgment and experience in this area is of relevance.
- Some threats affect data especially threats to physical assets such as fires, floods etc.
- Care needs to be taken in using any statistical threat data regarding the source of data; otherwise the analysis may be inaccurate or incomplete.
- In general, the greater the likelihood of a threat occurring, the greater is the risk. To some extent, the nature and value of information assets affect the likelihood of occurrence of a threat.
- If the asset is of high value, e.g. proprietary software packages, it is a prime target for piracy attempts.
- Thus, the identification and valuation of assets also assists with the identification of threats and their likelihood of occurrence.
- Periodically, the likelihood of occurrence of a threat needs to be reassessed due to changes occurring in the structure, direction, and environment of an organization.

(c) **Impact Analysis:**

- The threat that is successful in causing harm or loss to an asset results in an impact.
- Impact may be either in terms of direct loss of money or financial impact such as a hacker stealing a sensitive file containing all information about credit card customers that is used by the ATM access control system.
- Impact need not necessarily be in terms of direct impact of money; but can be, for example, disruption of operations leading to operational loss and delayed and back log processing etc.
- IT risks can also lead to significant losses in terms of damages (both monetary as well as to the reputation of the organization) such as a hacking attack leading to compromise of sensitive financial information of customers, which may be published by the hacker on the Internet resulting in both legal repercussions and loss of reputation.

Step 5: Developing Strategies for Information Risk Management

Once risks have been identified and assessed, appropriate corrections shall be made to the system, if required. Immediate action may not be taken to correct some identified vulnerabilities but the process will at least analyse these vulnerabilities, document and recognize them for risk management decisions.

Risk Management Strategies:

The strategies to manage the risk fall into one or more of these four major categories:

(a) **Risk Avoidance:** It means not doing an activity that involves risk. It involves losing out on the potential gain that accepting the risk might have provided. E.g. not using Internet / public network on a system connected to organisation's internal network, instead using a stand-alone PC for Internet usage.

(b) **Risk Mitigation / Reduction:** It involves implementing controls to protect IT infrastructure and to reduce the severity of the loss or the likelihood of the loss from occurring. E.g. using an effective anti-virus solution to protect against the risk of viruses and updating it on timely basis.

(c) **Risk Transfer:** It involves causing another party to accept the risk i.e. sharing risk with partners or insurance coverage.

(d) **Risk Retention / Acceptance:** It means formally acknowledging that the risk exists and monitoring it. In some cases it may not be possible to take immediate action to avoid/mitigate the risk.

All risks that are not identified or avoided or transferred are retained by default. These risks are called residual risks.

Risk management aims to identify, select and implement the controls that are necessary to reduce residual exposures to acceptable levels.

Risk Prioritization:

- The goals and mission of an organization should be considered in selecting any of these risk management strategies.
- It may not be practical to address all identified risks, so priority should be given to the risks that have the potential to cause significant mission impact or harm.
- In ideal information risk management, a prioritization process is followed whereby the risks with the greatest loss and the greatest probability of occurrence are handled first, and risks with lower probability of occurrence and lower loss are handled later.
- In practice the process can be very difficult, and balancing between risks with a high probability of occurrence but lower loss versus a risk with high loss but lower probability of occurrence can often be mishandled.

Understanding the Relationships Between IS Risks and Controls:

- Risks that threaten the IS cannot be altogether eliminated but, through appropriate decisions and actions can be mitigated.

  Threats to information system can materialize as an outcome of poor controls or absence of controls. Any threat to the system or its components could result in a loss to the company as a consequence of exploitation of the vulnerabilities.

  A control is a check or restraint on a system which is designed to enhance its security. Controls can act to

  - reduce a threat
  - reduce vulnerability to a threat
  - reduce impact of a threat
  - detect an impact
  - recover from an impact

- The objective of IS controls is to prevent the threats from exploiting the vulnerabilities of the assets or the safeguards.

  In the event the threats cannot be prevented, the controls should enable timely detection and trigger corrective action.

  In the event of failure of a control, threats could cause harm to the assets resulting in an actual impact.

- IS Auditor should be able to evaluate whether available controls are adequate and appropriate to mitigate the IS risks.

  In the case of deficiency in controls or existence of newer or uncontrolled risks, the IS auditor should report such weaknesses to the auditee management along with appropriate recommendations.

  Hence it is important for the IS auditor to understand the relationship between risks and controls. He should also be thorough with the process and procedure of reviewing and evaluating controls.

- The auditor should understand that the controls always have a *cost*, but also come with a *benefit*.

  The *cost* could be in terms of time or investment of money or sometimes even compromising with the performance of systems e.g. anti-virus software or intrusion detection systems consume the resources and might make the system slow.

  Benefits could be in terms of reduction of risk, or in terms of improving the effectiveness and efficiency of operations. In any organization, it is crucial to balance the cost vs. benefits of controls.

  The following rules apply in determining the use of new controls:

  - If control would reduce risk more than needed, then see whether a less expensive alternative exists.
  - If control would cost more than the risk reduction provided, then find something else.
  - If control does not reduce risk sufficiently, then look for more controls or a different control.
  - If control provides enough risk reduction and is cost-effective also, then use it.

No changes were found in any other chapter. These changes are as per study modules as on 23.01.2012.