ERP and CRM
(Assignment -II)

Submitted in partial fulfilment of the requirements for the degree of

Master of Technology in Information Technology

by

Vijayananda D Mohire

(Enrolment No.921DMTE0113)

Information Technology Department
Karnataka State Open University
Manasagangotri, Mysore – 570006
Karnataka, India
(2010)

ERP and CRM

CERTIFICATE

This is to certify that the Assignment-II entitled ERP and CRM, subject code: MT32C submitted by Vijayananda D Mohire having Roll Number 921DMTE0113 for the partial fulfilment of the requirements of Master of Technology in Information Technology degree of Karnataka State Open University, Mysore, embodies the bonafide work done by him under my supervision.

Place: ________________ Signature of the Internal Supervisor

Date: ________________ Name

Designation

Preface

This document has been prepared specially for the assignments of M.Tech – IT III Semester. This is mainly intended for evaluation of assignment of the academic M.Tech – IT, III semester. I have made a sincere attempt to gather and study the best answers to the assignment questions and have attempted the responses to the questions. I am confident that the evaluators will find this submission informative and evaluate based on the furnished details.

For clarity and ease of use there is a Table of contents and Evaluators section to make easier navigation and recording of the marks. Evaluator's are welcome to provide the necessary comments against each response; suitable space has been provided at the end of each response.

I am grateful to the Infysys academy, Koramangala, Bangalore in making this a big success. Many thanks for the timely help and attention in making this possible within specified timeframe. Special thanks to Mr. Vivek and Mr. Prakash for their timely help and guidance.

Candidate's Name and Signature Date

Table of Contents

Table of Figures

ERP and CRM

RESPONSE TO ASSIGNMENT – II

Question 1 How the information security is integrated in the ERP System?

Answer 1

It is important to understand how an ERP system is structured. This will ensure that the adapted security framework is mapped in a proper and consistent manner onto the ERP model. The ERP model consists of four components

1. **The Software Component** - The software component of the ERP model is the most visible to the users and is often seen as the ERP product. This includes modules such as General Ledger, Supply Chain management and Customer relationship management.
2. **Process flow** - The second component is the process flow within an ERP system. Process flow deals with the way in which the information flows among the different modules within an ERP system. This forms a very important part of understanding ERP systems.
3. **Customer mindset** - The third component addresses the resistance to change that could kill an ERP project. A proposed ERP system may hold great promise, but often fails to consider how the users are likely to view this so-called improvement
4. **Change management**- Change management plays a major role in the successful implementation of an ERP system and is the fourth component in the ERP model.

In addition to the above four Methodology component is also needed for proper integration of these four component.

The alignment of the ERP model and the security framework will enable an organization to implement an ERP System that will conform to international security standards. It will also ensure that once security is implemented, it will be ongoing function within the ERP system and will not be neglected. The three items of the Generic security framework (People, Policy and Technology) needs to be mapped to the above five ERP components. The details of these fifteen mappings are detailed in following sections.

Software component of the ERP model

1. **Policy component of the Security framework** – The policy component focuses on the policies and procedures that must be in place to manage and enforce security. Although the software component only deals with the software modules within an ERP system, CobiT and ITIL guide how the software is to be implemented. CobiT dictates to the Supplier Relationship Management (SRM) module how security must be managed with a customer. ISO 17799 affects the software module as follows:

   Security policy – A policy needs to be defined on how the ERP system will function and will include all relevant information.

   Asset classification and control– Although an ERP system is perceived as software, it also includes hardware and networking infrastructure. All these assets need to be classified and controlled. It also includes intellectual capital such as customization of the ERP system.

   Physical and environmental security– The physical ERP servers need to be hosted in a secure environment. Access to the system and premises must be controlled.

   Communications and operations– Operational procedures must be in place, e.g. the frequency of backups and the protection of the ERP system against unlawful access.

   Information access control –Access to the ERP system and even some modules and functions must be controlled

   System development and maintenance – This module will define the security within each software module and how the data will be encrypted

   Business continuity – The ERP system must be available for transacting and business continuity plans must be defined and tested to ensure that the ERP system can function in the event of a disaster

   Compliance– The ERP system must comply with standards and legalization.

2. **People component of the Security framework**: Although people are going to use the ERP system and will be affected by the security surrounding it, the software component is not affected that much by the people component. The issues influencing the people component are mostly soft issues such as trust and ethical conduct. The following are some of the hard issues involved:

   - Budget – The organization must spend money on training to ensure that the users of the ERP system understand how it works, the effect of security on their work and the issues surrounding ERP security.
   - Management – The users of the ERP system will only enforce security if it is encouraged by management
   - Change – The implementation of the ERP system will have an effect on the users since it will bring change into their lives. The organization must know how to deal with this change.

3. **Technology component of the security framework** – The seven pillars can be applied to the software component. The identification and authentication pillar determines who has access to the software components, while the authorization pillar determines the type of access to the software components, while the authorization pillar determines the type of access and the modules within the software component to which access is granted. The information supplied to the user by the software modules must be integrated as well as confidential. This means that information must flow from one side of the ERP system- such as the SRM module – right through to the printing of the invoice without any user intervention. It also means that special deals loaded by the supplier, for example, are not visible to outsiders and thus remain confidential.

Non-repudiation plays an important role; especially in the SRM and Supply chain Management (SCM) modules. All the software modules must always be available, especially for the interaction and flow of information between the different modules, as well as for customer and supplier convenience. All aspects must be auditable and it is very important that the software comply with auditing standards.

Customer Mindset component of the ERP model

1. **Policy component of the security framework** – The policies and standards of the organization will have an effect on how users perceive the ERP system. The users should not perceive security as a burden, but rather as a necessity to ensure the integrity and confidentiality of information. A few modules of ISO 17799 play a role in the customer mindset component. One is the security organization, another is the personal security module that determines who get employed.

2. **People component of the security framework** – The people component and the customer mindset both deal with the way the user interacts with the ERP system. These two components influence each other and are interdependent. A comparison of the two follows:
    - Policy and procedures – The policy and procedures instilled by the organization will influence the employees of the organization. The way they work will be governed by the policies and procedures.
    - Benchmarking – The organization can use benchmarking to compare itself to other organizations. This comparison will enable the organization to determine where it is lacking in security and how it measures as an organization in terms of the rest of the industry.
    - Risk analysis – The employees of the organization must be involved in the day-to-day risk analysis. This will ensure that security policies are up to date and will make users aware of any security breaches.
    - Budget– The organization must train the users in the impact of security on their lives and the way they work. The implementation of security affects the way users work and interact with the ERP system, so the budget should allow for education in this regard.
    - Management – The management of the organization should make security a way of life by enforcing and implementing it themselves.
    - Trust – The users of the ERP system must be trusted by the organization to interact with the ERP system and to enforce the security rules and regulations
    - Awareness – The users must be aware of how confidential, integrity and availability are impacted if they do not abide by security policies.
    - Ethical conduct – The integrity of the ERP system will be affected by the ethical code and conduct instilled by the organization. For example, users must be aware that they cannot work on the information from home.

3. **Technology component of the security framework**- Identification and authentication play a vital role in the customer mindset component. If the users do not abide by the rules of the technology component, the security will have no effect. For example, the users must understand what the consequences are if they pass their username and password on to someone else. This also affects the authorization pillar and the consequences can be far- reaching. The ERP system must also be audited to ensure that the users comply with the policies and procedures of the organization. The ERP system cannot be implemented within an organization if change does not take place.

Change management component of the ERP system

Change management not only deals with the changes that the ERP system enforces on the organization, but also with system changes once the system is implemented and business process changes.

1. **Policy component of the security framework** - Changes to the ERP system cannot be made without considering the policies and standards of the organization. The deployment of new versions of software will be managed by ITIL, which will ensure a smooth upgrade. During the lifetime of an ERP system, the business process will change, having an impact on security. ISO 17799 plays a role in the implementation of the ERP system and will manage the security aspects during the changes that are instilled by the system. Changes to the security policies will be addressed by the security policy component and the new roles and responsibilities will be addressed by the security organization component.
2. **People component of the security framework** - Certain aspects of the people component have an impact on the change component of the ERP model. Policies and procedures will change during the implementation of an ERP system and awareness regarding the system will change to accommodate new ways of doing things. The management of the organization must also ensure the users are aware of these changes to the policies and the necessary education must be provided.
3. **Technology component of the security framework** - System and business process changes have an effect on the following four pillars:

    - Confidentiality - The system or business process changes must not affect confidentiality. The information must still only be accessible to authorized users
    - Integrity - The information must not be compromised during changes and must still be intact after the changes to the ERP

system

- Availability – The ERP system must be available for transacting, which makes it difficult for system administrators to implement changes. Careful planning is needed to minimize the effect of downtime
- Auditing – After system or business process changes, the ERP system must still pass all audits

Process flow component of the ERP system

The process flow component of the ERP system deals with the way information flows between the different software modules

1. **Policy component of the security framework**- ISO 17799 will affect the way the different components interact with each other. It will also determine the level of information that flows between the different software components.
   a. Asset classification and control- This component will determine the protection between the different modules and will ensure that the different software modules do not influence each other in a negative way.
   b. Communications and operations – During the flow of information between the different modules, this component will provide the guidelines to ensure that the information is intact and not tampered with.

An aspect that must be considered during the process flow is the access control and the system maintenance of the ERP system.

2. **People component of the Security framework:** The people component does not play a significant role because all information flow happens in the background of the ERP system. The only aspect that must be taken into considerations is that the users must be aware of how the system works and the impact their actions might have later on.

3. **Technology component of the security framework:** The flow of information between the different software components must be controlled by the following pillars:
   - Confidentiality – Information should remain confidential as no user directly interacts with the information as it flows from one module to another. The less user interaction, the better the confidentiality of the

information.

- Integrity - The information that flows from one software module or even within a module must be the same when it reaches its destination. The information must not be altered during the process flow.
- Availability- The ERP system must be available to ensure that information can flow between the different modules. If some modules are not available, it can lead to corrupt data or the recapture of data.

Methodology component of the ERP system

1. **Policy component of the security framework** - It is the responsibility of the program manager to ensure that CobiT and ITIL are adhered to during and after the implementation of the ERP system. This adherence to international standards and guidelines ensures that customers are content to deal with the organization because they know that the organization and systems are adhering to the standards. The policies of the organization take precedence over the policies of the ERP system, that is, the ERP system must be adapted to accommodate the policies of organization and not the other way around.
2. **People component of the security framework** – The people component will determine who within the organization is responsible for the security aspects of the ERP system. These responsibilities will be derived from the overall people component of the security framework and will be incorporated into the ERP system security. If a person's responsibility is to implement password policies for the organization, then the same person must be responsible for the password policies of the ERP system. The program manager responsible for the implementation of the ERP system must ensure that all the relevant people are involved and incorporated into the project team. This will facilitate security being implemented from the beginning of the implementation and not just as an afterthought.
3. **Technology Component of the security framework** – The seven pillars of ERP security must be incorporated in the ERP system. These pillars form the foundation of ERP security and determine what users and customers are allowed to do within the system. These pillars also ensure that the confidentiality, integrity and availability of the information are above suspicion. The program manager must ensure that these pillars are addressed during the design of the ERP system and that they form part of the overall project plan. The seven pillars must be part of the design and process flows of information between the different software modules.

Evaluator's Comments if any:

Question 2 What are the main reasons for adopting CRM?

Answer 2

Competition for customers is intense. From a purely economic point of view, firms learned that it is less costly to retain a customer than to find a new one. The oft-quoted statistics go something like this:

- By Pareto's principle, it is assumed that 20% of a company's customers generate 80% of its profits
- In Industrial sales, it takes an average of 8 to 10 physical calls in person to sell to a new customer, 2 to 3 calls to sell to an existing customer.
- It is 5 to 10 times more expensive to acquire a new customer than obtain repeat business from an existing customer. For example, according to Boston Consulting Group, the costs to market to existing Web customers is $6.80 compared to $34 to acquire a new Web customer.
- A typical dissatisfied customer tells 8 to 10 people about his or her experience. Although often repeated, sources for many of these numbers could not be found.
- A 5% increase in retaining existing customers translates into 25% or more increase in profitability

In the past, the prime approach to attracting new customers was through media and mail advertising about what the firm has to offer. This advertising approach is scattershot, reaching many people including current customers and people who would never become customers. For example, the typical response rate from a general mailing is about 2%. Thus mailing a million copies of an advertisement, on average yields only 20,000 responses.

Another drive is the change introduced by electronic commerce. Rather than the customer dealing with a salesperson either in a brick and mortar location or on the phone, in electronic commerce the customer remains in front of their computer at home or in the office. Thus, firms do not have the luxury of someone with sales skills to convince the customer. Whereas normally it takes effort for the customer to move to a competitor's physical location or dial another 1-800 number; in electronic commerce firms face an environment in which competitors are only a few clicks away.

The most forward-thinking companies have recognized from past failures that CRM smacks of strategy, and thus technology alone can't address high-profile issues such as new-customer acquisition and Web-based marketing. To these companies, CRM is much more than a standalone project accounted for by a single organization, it's a *business philosophy* that affects the company-at-large. (We'll see examples later of companies who practice CRM without even using the term.) These firms have articulated their ultimate visions for CRM to communicate them to every facet of operations. The following list represents a set of legitimate CRM business objectives from several of my clients currently in the throes of their CRM programs:

- "We want to thoroughly understand our customers' needs—even before they know them themselves."—A mid-market financial institution
- "Decreasing customer churn by increasing customer satisfaction."—A competitive local exchange carrier
- "Motivating customers to initiate revenue-generating contacts with us."—An online insurance company
- "Increasing the likelihood of the 'right response' by a given customer or customer segment."—A catalog retailer
- "To use technology to improve customer service and enable a greater degree of customer differentiation in order to deliver unique customer interactions."—A data services firm
- "We want to attract customers—both old and new—through more personalized communications."—An online retailer

The point here is that there are not one but many visions for CRM success. CRM promises to help companies get to know their customers well enough to understand which ones to keep and which ones they should be willing to lose—and why—and how not to overspend in the meantime. CRM also means automating many of the business processes and accompanying analysis and saving precious time in the bargain.

And saving money. Charles Schwab's multimillion-dollar investment in Siebel's CRM product, which the brokerage firm uses to track each interaction with a customer or prospect, was recouped in less than two years. Stories of wildly successful CRM programs have invaded print and cyberspace, spurring otherwise cynical executives to turn their heads in the CRM direction. After all, who could argue?

Operational aspects aside, CRM is first and foremost a business strategy, one that helps a company tighten its business practices across organizations while forging an ironclad connection with its customers. It is not only a response to competitive pressures facing every industry—from deregulation to supply-chain efficiencies to the massive demand for Web-based customer interaction—it is also considered a strategic imperative, garnering executive-level attention and equally lofty budgets.

In the business-to-consumer (B2C) space, CRM means keeping pace with a savvy and increasingly impatient consumer base that is closer than ever to finding your main competitor and more willing than ever to share their bad experiences with your prospects. Making it all work together and seamlessly involves nothing short of organizational choreography.

That CRM is a business strategy is now a well-worn maxim. That it involves much more than information technology is sometimes disheartening news to many a manager gunning for that elusive quick win. The CRM best-practice company is the one that understands how to improve business practices and customer relationships by using CRM technology and customer data as part of an overarching program that also involves process and organizational changes, with the ultimate aim of differentiating itself through superior customer relationships.

Two main types of CRM that help realise the dream are “operational” and “analytical” CRM. The distinction is an important one, because it speaks to the tactics a company is taking in implementing its CRM strategy

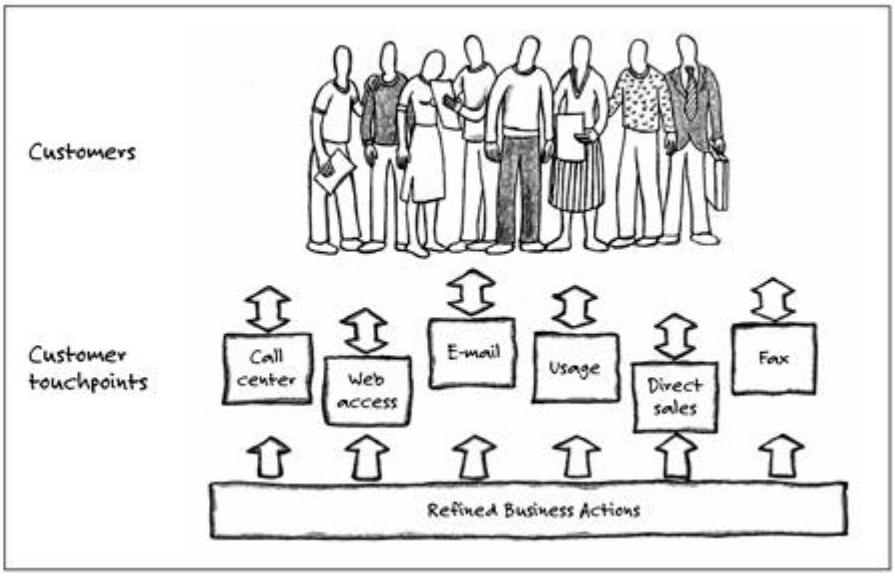


Figure 1 Operational CRM

Operational CRM, also known as “front-office” CRM, involves the areas where direct customer contact occurs. We'll refer to these interactions as customer “touchpoints.” A *touchpoint* can be an inbound contact—e.g., a call to a company's customer support hotline—or an outbound contact—e.g., an in-person sales call or an e-mail promotion. The majority of self-described CRM products on the market today fall into the operational category. Figure 1 illustrates the various levels of operational CRM.

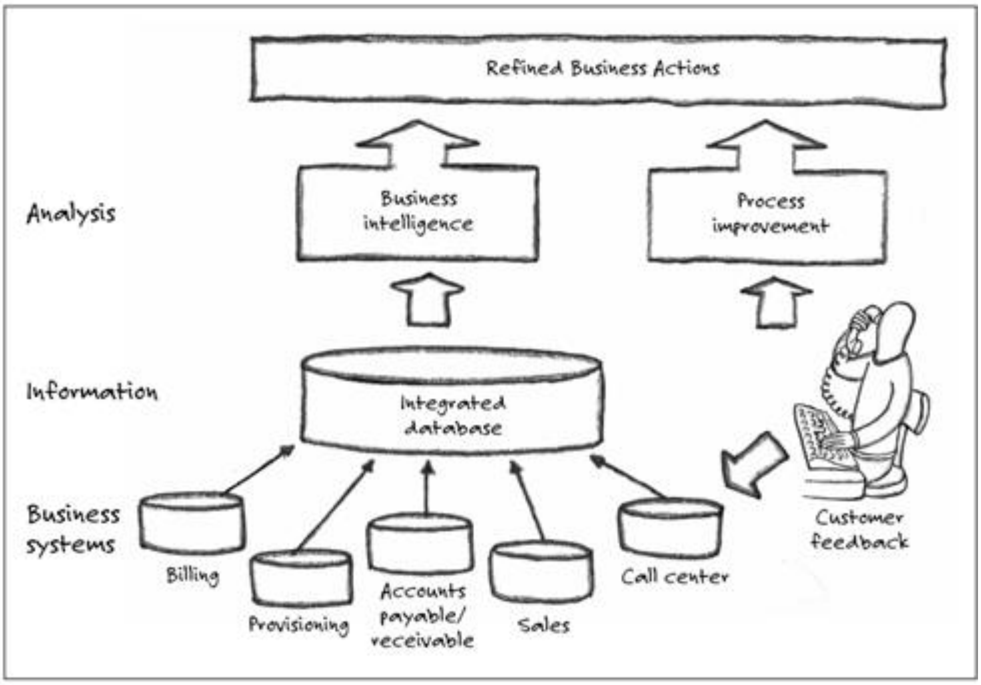


Figure 2 Analytical CRM

Analytical CRM, also known as “back-office” or “strategic” CRM involves understanding the customer activities that occurred in the front office. Analytical CRM requires technology (to compile and process the mountains of customer data to facilitate analysis) and new business processes (to refine customer-facing practices to increase loyalty and profitability). Under pressure from analysts and industry experts, most of today's CRM vendors are either creating analytical CRM capabilities or partnering with business intelligence (BI) vendors to incorporate analysis into their offerings. Figure 2 shows how the data and processes combine to refine business actions.

Company types that must adopt CRM

Companies that do not repeat business from customers will not gain much of CRM. And also that have walk-in customers not providing multiple sales and services channels will not benefit much from CRM. Again if maintaining long term relationship with customer is not a priority for the company. It will be wise not to invest in CRM.

Then who benefits? The more the channels to access customers and more the number of touch points with customers, greater is the need for CRM installation. Companies in

- Banking
- Finance
- Insurance
- Airlines and hotels
- Telecommunications and health care benefit from installing CRM software

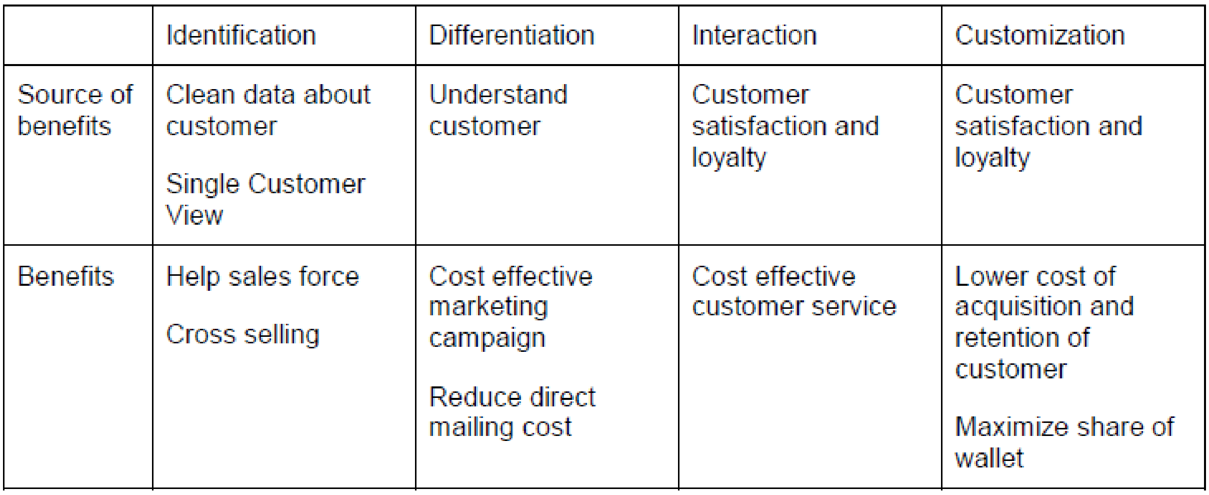
The principal benefits of CRM are to

- Improve the organization’s ability to retain and acquire customers
- Maximize the lifetime value of each customer (share of wallet)
- Improve service without increasing cost of service.

Some of these benefits can be measured and others cannot.

To obtain all of these benefits, sales, marketing, and service functions need to work together. The benefits are shown in Table 1

Table 1 Benefits of CRM project



	Identification	Differentiation	Interaction	Customization
Source of benefits	Clean data about customer Single Customer View	Understand customer	Customer satisfaction and loyalty	Customer satisfaction and loyalty
Benefits	Help sales force Cross selling	Cost effective marketing campaign Reduce direct mailing cost	Cost effective customer service	Lower cost of acquisition and retention of customer Maximize share of wallet

Evaluator's Comments if any: