NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

STRUCTURED MANAGERIAL APPROACH TO DECISION PROCESSES SHAPING INFORMATION TECHNOLOGY IN NON-IT ORGANIZATIONS

by

Gabriel V. Ana

June 2000

Thesis Advisor: William J. Haga
Associate Advisor: Roger Evered

Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	June 2000	Master's Thesis

4. TITLE AND SUBTITLE :
Structured Managerial Approach to Decision Processes Shaping Information Technology in Non-IT Organizations

5. FUNDING NUMBERS

6. AUTHOR(S)
Gabriel V. Ana

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES
The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT

This thesis' purpose is to address the inter-disciplinary area of managerial decisions concerning IT structures in non-IT organizations. It is neither intended as a review of general managerial theory, nor aimed at the technical aspects involved. It rather approaches the IT support implementation and revising from a practical managerial perspective, attempting to systematize and streamline the decision-making process. Both managerial theory and technological dimension are considered equally important, but called upon only when and at the necessary extent they are required to lay the basis for making decisions.

Between the large knowledge base in the managerial field on one hand, and the newer but dynamic IT-related sciences on the other, there is a gray area avoided by both management scholars and computer scientists. The first group sees IT as merely a tool, without accepting they have to deal with the transformational effect of technological developments. It is characteristic for the exponents of this school to label IT people as "technical" and to discount the specific impact of this particular technology on organizations. The second group, in a continual effort to keep up with the technological boom, is drifting away from the social and organizational issues of IT to focus on the technical side, without acknowledging other managerial dimensions than the one centered on the IT structures *as its object*. Both sides tend to focus research in their respective areas, leaving managers of non-IT organizations with an inadequate choice between the two approaches. This thesis is aimed towards bridging the resulting inter-disciplinary gap with a flowchart model for the decision process in the analyzed area, using as modules applicable techniques and methods from both managerial and computer science fields, presented in practical operational form.

14. SUBJECT TERMS
Information Systems, Management, IT Support, Internet, Networks

15. NUMBER OF PAGES
200

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

STRUCTURED MANAGERIAL APPROACH TO DECISION PROCESSES SHAPING INFORMATION TECHNOLOGY IN NON-IT ORGANIZATIONS

Gabriel V. Ana
Major, Romanian Air Force
B.S., Technical Military Academy, Bucharest, 1983
B.A., Academy of Economic Studies, Bucharest, 1993

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
June 2000

Author: _____
Gabriel V. Ana

Approved by: _____
William J. Haga, Thesis Advisor

_____
Roger Evered, Associate Advisor

_____
Reuben T. Harris, Chairman
Department of Systems Management

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis' purpose is to address the inter-disciplinary area of managerial decisions concerning IT structures in non-IT organizations. It is neither intended as a review of general managerial theory, nor aimed at the technical aspects involved. It rather approaches the IT support implementation and revising from a practical managerial perspective, attempting to systematize and streamline the decision-making process. Both managerial theory and technological dimension are considered equally important, but called upon only when and at the necessary extent they are required to lay the basis for making decisions.

Between the large knowledge base in the managerial field on one hand, and the newer but dynamic IT-related sciences on the other, there is a gray area avoided by both management scholars and computer scientists. The first group sees IT as merely a tool, without accepting they have to deal with the transformational effect of technological developments. It is characteristic for the exponents of this school to label IT people as "technical" and to discount the specific impact of this particular technology on organizations. The second group, in a continual effort to keep up with the technological boom, is drifting away from the social and organizational issues of IT to focus on the technical side, without acknowledging other managerial dimensions than the one centered on the IT structures as its object. Both sides tend to focus research in their respective areas, leaving managers of non-IT organizations with an inadequate choice between the two approaches. This thesis is aimed towards bridging the resulting inter-disciplinary gap with a flowchart model for the decision process in the analyzed area, using as modules applicable techniques and methods from both managerial and computer science fields, presented in practical operational form.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF ABBREVIATONS, ACRONYMS AND SYMBOLS

IT	Information Technology
ACL	Access List Control
ACS	Access Control System
API	Application Program Interface
ATM	Asynchronous Transfer Mode
BER	Bit Error Rate
BRI	Basic Rate Interface
CAD	Computer-Assisted Design
CBT	Computer-Based Training
CER	Cell Error Rate
COTS	Commercial Off The Shelf
CPU	Central Processing Unit
CSMA/CD	Carrier Sense, Multiple Access / Collision Detect
DBMS	DataBase Management System
DFARS	Defense Federal Acquisition Regulation Supplement
DoD	Department of Defense
DoS	Denial of Service
DSL	Digital Subscriber Line
DSN	Data Name Service
EIS	Executive Information Systems
FAR	Federal Acquisition Regulation
FBI	Federal Bureau of Investigation
FDDI	Fiber Distributed Data Interconnect
FEDSpecs	Federal Specifications

FIFO	First In First Out
FTP	Foil-shielded Twisted Pair
GSA	General Services Administration
HRM	Human Resource Management
HRMS	Human Resource Management System
HTTP	Hyper Text Transfer Protocol
IETF	Internet Engineering Task Force
IMS	Inventory Management System
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISP	Internet Services Provider
ITS	Information Technology Support
LAN	Local Area Network
MAN	Metropolitan Area Network
MILSpecs	Military Specifications
MTBF	Mean Time Between Failures
NASA	National Air and Space Agency
NPV	Net Present Value
OC-3	Optical Carrier (throughput 3 = 155.52 Mbps)
OC-48	Optical Carrier (throughput 48 = 2.488 Gbps)
OS	Operating System
OWS	Organizational Web Site
PD	Purchase Description
PGP	Pretty Good Privacy
PMS	Process Monitoring System

PRI	Primary Rate Interface
PVC	Permanent Virtual Circuit
R&D	Research and Development
RDMBS	Relational DataBase Management System
ROI	Return On Investment
S-HTTP	Secure Hyper Text Transfer Protocol
SLA	Service Levels Agreement
SMDS	Switched Multimegabit Data Service
SONET	Synchronous Optical Network
SPEC	Standard Performance Evaluation Corporation
SSL	Secure Sockets Layer
T-1	Dedicated line (1.544 Mbps)
T-3	Dedicated line (43 Mbps)
TCO	Total Cost of Ownership
TCP/IP	Transfer Control Protocol / Internet Protocol
UTP	Unshielded Twisted Pair
VPN	Virtual Private Network
WAN	Wide Area Network

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

We all live in a wired world. It is an inescapable fact of life, and ignoring it doesn't change the pressure of emerging technologies on each and every organizational aspect managers have to deal with. Communications and information technology literally change the way we live, work and spend our spare time. Traditional organizational management is under siege at every level, from its conceptual basis to the most common decision-making processes it includes, because it deals with information, and this is all IT is about. Books have been written and scholar effort spent in an effort to identify the best ways an organization should cope with both environmental change and internal pressures for improvement, but IT has seldom been their focus, although its role as the plumbing system for the information flows became undeniable. Therefore, in my view, there is no escape to the need to put IT-related concerns in their right place in managerial endeavors, and this can only be achieved by unveiling a managerial perspective on this issue.

This study is but a starting point in an effort to filter, sort and clarify what managers should know when trying to cope with change in organizational IT. A high enough level of generality was sought, in order to cover non-IT organizations regardless of their specifics. This also means most concepts used here need to be refined and particularized to reflect actual conditions and become an actual decision-making tool. However, the main result targeted by this study is to systematize and organize IT-related managerial concerns in a structured template, which can constitute the basis for understanding, designing, implementing and controlling the change in this field, without loosing the big picture because of complex technical issues.

Two things can happen if the need for structuring and integration of IT knowledge at managerial level is not given the proper consideration. First, because of the continuing and rapid evolution of this industry, technology gets more and more complex and drifts away from the area managers include in their information basis for decision-making. In other words, the more you wait, the harder it gets to understand IT as it becomes increasingly esoteric. Second, as IT people have a difficult task to keep up with rapid technological developments, they loose business objectives from their focus and concentrate on exciting new technical features, which may bring nothing to the organization. Once managers and IT people contemplate organizational IT from completely separate perspectives, then ITS ceases to add value and may become an erratic source of trouble, sinking money into useless technology and wasting organizational efforts to no avail.

Three major sources of information were used in this study to draw upon and integrate useful information: 1) management and computer science textbooks, 2) mass media, including computer magazines and online publications and 3) the author's own experience in managing large IT acquisition programs. The sheer volume of information available on IT and management makes each of these fields unmanageable as such, to provide the theoretical basis for a concrete project. When compared, the two domains talk about the same issues using different terms and completely separated approaches. For example, the steps to be taken in setting up a new IT system are focused on technical requirements in computer science literature, while managerial approaches stress the business side and give scanty, if any, consideration to aspects like data security, web site or e-commerce. Therefore, the study is focused on the gap between the two domains and

draw from both to bridge it with a set of concepts, methodologies and approaches to the questions facing managerial decision-making, in an attempt to put order and help managers maintain control over IT changes in non-IT organizations.

Criteria used to filter information and choose the appropriate level of concept complexity included in the study were based on the assumption that managers don't need to review the managerial theory and, in fact, have no time to do so for every project they look at. All they need is a sense of the specific areas they need to focus on in IT projects and a list of risks and benefits associated with available alternatives. Consequently, each chapter looks at a specific area of concern and offers two types of results: a summary of knowledge necessary to understand the concepts and ask the right questions and a structured approach to the issue at hand.

Chapters are organized according to the logical flow of information needed in the process of implementation of a new IT system. However, for practical purposes they can be read separately or in a sequence that best mirrors the actual process the information is needed for. Supplementary information is included in annexes and references can provide a more detailed look to specific issues.

THIS PAGE INTENTIONALLY LEFT BLANK

II. IT SYSTEMS LIFECYCLE

A. SPECIFICS OF IT LIFECYCLE

Generally speaking, an IT system has a lifecycle similar to any complex industrial system. It typically includes a concept phase, requirements phase, design phase, implementation phase, test phase, installation and checkout phase, operation and maintenance phase (with or without a number of upgrades), and eventually the retirement phase. However, several aspects that are unique to IT require managerial consideration:

- The scope of IT services in an organization is seldom restricted to a particular operation, department or geographical area. It rather encompasses a multitude of functions spread across the whole organization.

- IT is inherently programmable. Therefore, the actual uses to which it will be put are unpredictable.

- The high rate of change, as a result of both technological obsolescence and external pressures makes IT systems dynamic and evolutionary, even between major transitions to new technologies. Upgrading is a continuous process, as software enhancements and hardware improvements become available frequently from the producers, and compatibility requirements press to keep up with the general trends.

- Sub-systems have their own lifecycles, but partial modifications or upgrades affect the overall performances. For example, a network cabling subsystem with a technical life span of ten years can support several generations of workstations or peripherals without modifications and, once upgraded, the whole system benefits from the newly gained features.

- ITS emulates and carries the information flows in the organization. It must closely reflect the specific paths and formats used by the processes it supports. Even the most comprehensive off-the-shelf solution needs to be thoroughly customized to fit the actual needs of the organization. As a result, there are no identical ITS implementations, no matter how similar the respective organizations may be. This creates the need for configuration management.

- While short-term needs, required budgets, and available technologies for ITS can be predicted with a fair degree of accuracy, long-term forecasts are affected by the inherent uncertainty of this volatile industry. This hinders planning efforts, especially for longer time horizons, such as the lifecycle of ITS.

- Dynamic evolution of IT limits the possibility of newer implementations to draw heavily on the experience previously gained with similar systems. As a result, much of the initial phase of the lifecycle are based on experiments, mounted to test and validate requirements or possible solutions.

Literature in this field identifies and describes a multitude of models used to cope with IT lifecycle:

- The Waterfall Model
- The Putnam Waterfall Model
- Incremental Model
- Linear and Non-linear Models
- The Prototyping Model
- Evolutionary Model

- The Military Standard Model
- Hardware and Software "V" Model
- Spiral Model
- Object-oriented Model
- The Novell Model

Descriptions and further information on these models can be found at International Society of Parametric Analysts [Ref. 20] and NASA [Ref. 24].

Each model eliminates some aspects, seen as irrelevant to the analysis, and stresses others considered important. Because lifecycle models are theoretical instruments used to create a basis for practical approach to program or project management, each concentrates on the segment of time or set of functions that are important to the specific activity that needs to be planned. For example, NASA's DSN Software Engineering Guidebook adopts the Waterfall model and the Spiral model as best suited for the software development process.

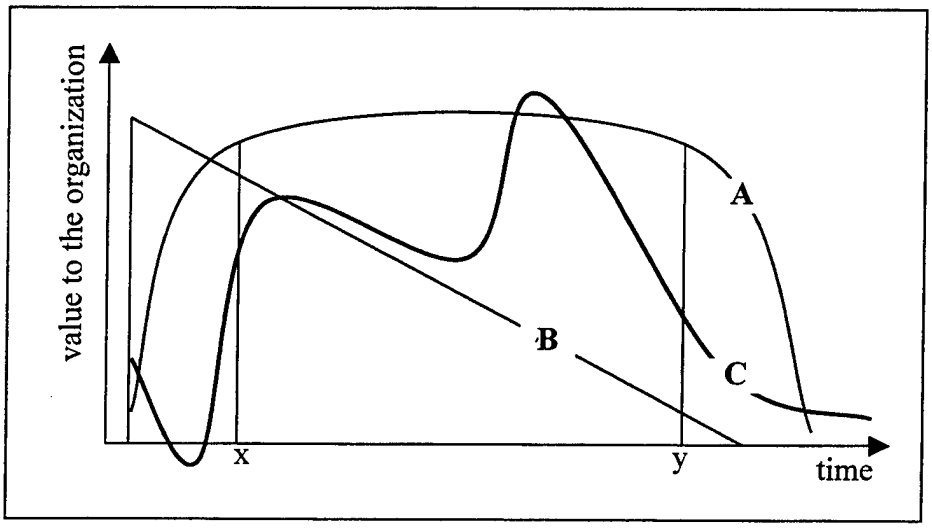

Figure II-1

Three diagrams are shown in Figure II-1 to illustrate differences between models used for lifecycle value estimation. Curve A is the traditional lifecycle "organic " model for industrial systems. Curve B represents the linear model used for asset depreciation in the accounting systems of many organizations. Curve C reflects my personal experience in IT systems development.

The organic model defines an initial growth phase (before point x), a useful life phase (between points x and y) and eventually a decay / retirement phase (beyond point y). More elaborate variants of this model also emulate small variations during the useful life phase, due to either learning curve effects or gradual devaluation produced by obsolescence and declining performances.

Straight-line depreciation used in accounting models is just one of the possible formulas, used here to illustrate differences and contrast assets accounting data with actual benefits of the IT system for the organization.

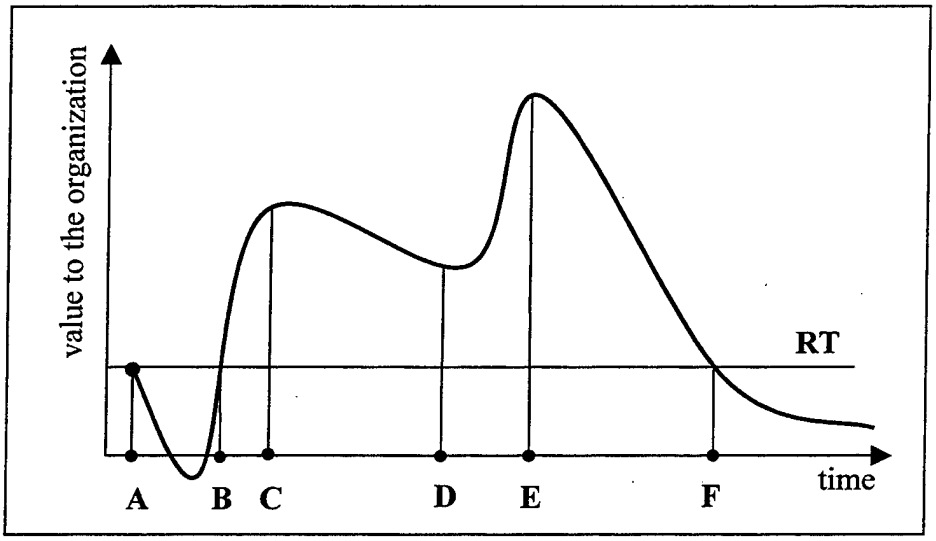

Figure II-2

The third curve, detailed in Figure II-2, is an adapted version of the spiral model, including the effects of phenomena like initial investment, upgrade(s) and asymptotic residual value of IT equipment and software.

This model defines seven successive milestones in the life of an IT system, starting with the moment the first monetary unit is spent on building the concept or identifying whether change is necessary (see chapter III), and ending at the time the market value of the existing IT goes below its return threshold (RT). RT is the minimum level of benefit to the organization where the current IT system usage is still justified. The value of ITS for the organization is considered here to be the aggregated benefits, both tangible and intangible, induced by the respective implementation. See chapter VI for a discussion on measurability of ITS benefits.

Between milestones A and B, the new IT system is a resource consumer, and its return on investment is negative. The actual depth and duration of this initial net loss depends on factors like:

- Complexity of the change.
- Number of sites and workplaces per site.
- Local and remote throughputs needed.
- Criticality of the applications implemented.
- Strength of the security system used.
- Outsourcing arrangements.
- Urgency or other constrains on the process of IT change.
- Previous expertise in orchestrating major changes.

Since planning and budgeting for the project need to work with estimations of time and costs for each phase, including the initial interval between milestones A and B, two groups of sources can be used to find a basis for that kind of data: 1) external sources and 2) internal sources. The former group includes technical specifications, catalogues, reports, reviews, presentations, press releases and so on, highlighting performances and results of similar or partially similar implementations in other organizations. Variances and uncertainties related to this group of sources are discussed in more detail in chapter XII. The latter group is largely based on requirements, but it is a good idea to use reduced-scale models and experiment concepts and solutions every time this approach is practicable, because the farther basic data is from the reality it reflects, the higher its degree of uncertainty. For example, norms and standards built on statistics and used to estimate labor cost in ITS may be a good source for planning and budgeting, but a reduced-scale experimental module emulating the real system can offer more relevant data if the survey is conducted properly.

Between milestones B and C the system already produces more benefit than it costs the organization. Cumulated effects of the learning curve and gradual elimination of transient technological hitches brings the system to its peak effectiveness and efficiency at milestone C. The shorter this interval the better, because protracted implementations run against external competitors who may not have the same problems and, although productive, this interval is not efficient.

Between milestones C and D the system provides the services at the quality and quantity required, but its value to the organization declines, as technological resources of equipment are depleted and obsolescence starts to affect effectiveness. Just how steep this

process is, depends on the actual system's structure, characteristics and role. A simple IT system, with relatively high performances to begin with, and used for secondary purposes in the organization will display a flatter curve than a system with features at the opposite ends of the spectrum.

The interval pictured between milestones D and E is an upgrade. Several such intervals can be successively included in the model, depending on the actual number of such processes the system goes through. At the simplest level, an upgrade may be aimed to restore the original performances with newer — and sometimes more effective — equipment or software. However, upgrades can and are used also to enhance original performances in order to take advantage of newly offered features or to meet added requirements.

Between milestones E and F the system is at the end of its economic life, no upgrades are available or justifiable, but benefits produced still overcome costs. Keeping it in use — sometimes against the suggestions of IT people that are usually anxious to take the next technological step — is economically justified, saves money and gives time to prepare the next change. The slope of this segment is strongly influenced by external developments. By this moment, the system closely identified itself with the organization and the need for change is more externally induced than internally welcomed. See chapter XI for a more detailed discussion on IT effects on the organization.

Beyond the milestone F the system becomes a problem. Although its value doesn't drop to zero because there are functions it can still perform, keeping it in use means more costs than benefits. Good management of IT forecasts this moment and set in

motion the next lifecycle so as to synchronize the point B for the new system with the point F for the new one. See a discussion of this issue in chapter IV.

B. LIFECYCLE BUDGETING

One of the main purposes of IT lifecycle models is to provide a basis to allocate and manage resources and track results using financial references and indicators, i.e. to budget for IT. Keeping in mind the considerations discussed in the previous section and translating variations of value into budgetary items, it becomes apparent that a lifecycle spanning over several years will not yield identical or even similar budgets year after year. Moreover, sub-systems of ITS have their own lifecycles and organizational IT budget, as a planned sum of individual outlays and financial sources reflects all individual variations in an aggregate form. To illustrate this concept let us consider Figure II-3.

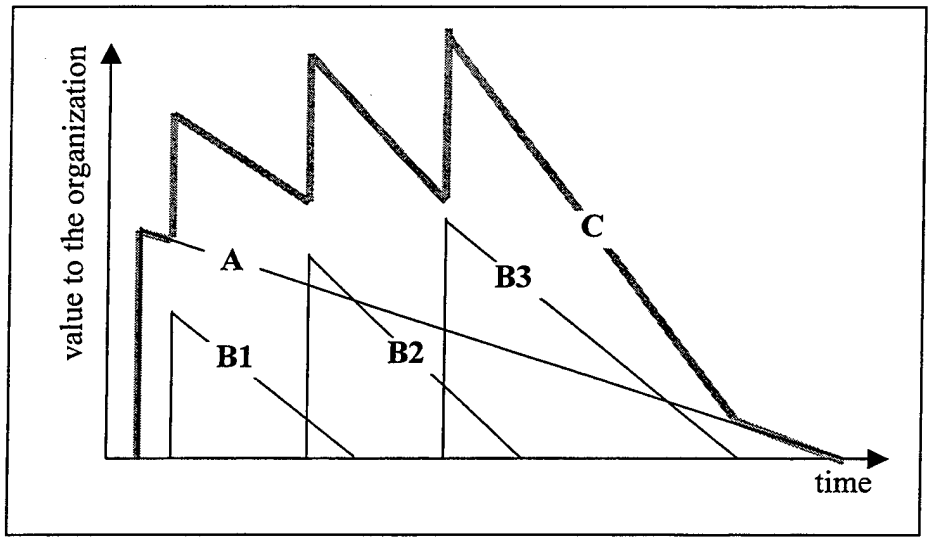

Figure II-3

Curve A represents the value of an IT asset with a long lifecycle — for example network cabling — described using one of the simplest asset accounting models: the straight-line depreciation formula. Curves B1, B2 and B3 represent successive

acquisitions of other IT assets included in the system — for example desktop computers — which have shorter lifecycles and use here for simplicity the same accounting model. Curve C sums the value of the entire system, as it is reflected in the balance sheet. The aggregated value does not respect the same variation pattern as the basic components. A simple mental exercise can expand this conclusion to a larger number of different items, described by complex lifecycle models, and integrated in ITS. This not only explains overall variations in required budgets for IT, but also recommends the usage of a comprehensive model to identify the actual position of the current system in its lifecycle.

The main steps to be taken for building a relevant IT budget depend on the specific activities supported by IT and the profile of the organization. Here is a possible template for the budgeting process (adapted after Sewell and Marczak, [Ref. 26]):

- Step 1: Define initial requirements — discussed in chapter IV.
- Step 2: Determine the duration of the need for each of the functional goals.
- Step 3: Identify the full range of technologies required for the success of the project: network hardware, network-based services, desktop hardware, shared peripherals, maintenance, training, technical support and so on.
- Choose the lifecycle model that best fit each category used in the budget and identify its milestones.
- Step 4: Assign life-cycle measures to each of the technologies in your budget, for example:
    - Personnel costs: annual .
    - Service contracts and licenses: annual or as contracted / forecasted.

- Maintenance costs: annual or as specified for each category.
- Software: 1-3 years.
- Hardware: 2-5 yearsWiring: 5-15 years.

- Step 5: Use a life-cycle budget worksheet to estimate annual costs of the project for its duration, compounding annual costs computed for each category with the formula:

annual cost = total cost / life cycle years, or

- Step 5a: Aggregate annual figures for all categories into the overall project budget.

Budgeting process for IT is not conceptually different from similar processes used for other technology-based projects. What is different here comes from specific traits of IT lifecycle discussed in the previous section.

Once this phase is concluded, the resulting financial image of the project can be used in the decision workflow described in chapter IV, to support the necessary trade-off between needs and resources. In order to become a managing tool, this provisional budget needs to be 1) completed with the timetable of resource availability — matched against the financial outflows — and 2) included in a periodical or milestone-based revision process.

III. INITIAL ANALYSIS: IS *ITS* CHANGE NECESSARY?

For any organization that is not in the business of providing Information Technology (IT) products and/or services, IT Support (ITS) is used to add value to operational and support divisions or functions. Along with marketing, accounting, maintenance, and human resources, ITS is a service provider for the organization, regardless of the underlying structure — a distinct ITS division or distributed elements included in the functional compartments. Since ITS is a function within the organization, its effectiveness, efficiency and contribution to the general organizational objectives should be identified, measured, compared against internal and external reference values, and assessed in order to determine whether it meets requirements and expectations or there is need for change. The issue of measurability for this particular area of service — subject to contradictory points of view — is discussed from a managerial perspective in section VI.A. For the purpose of the present discussion, let us consider ITS costs and benefits measurable.

The kind of change considered in this process refers to major modifications of structure and functionality of ITS implemented in order to enhance and/or gain new capabilities.

A. DECISION FLOWCHART

Initial analysis is not a step, but a continuous process. It consists of a set of comparisons between indicators reflecting external IT environment and internal ITS. The general objective is to answer the question whether existing ITS needs a major change in order to fulfill its designated role within the organization.

A conceptual diagram of this process is presented in Figure III-1

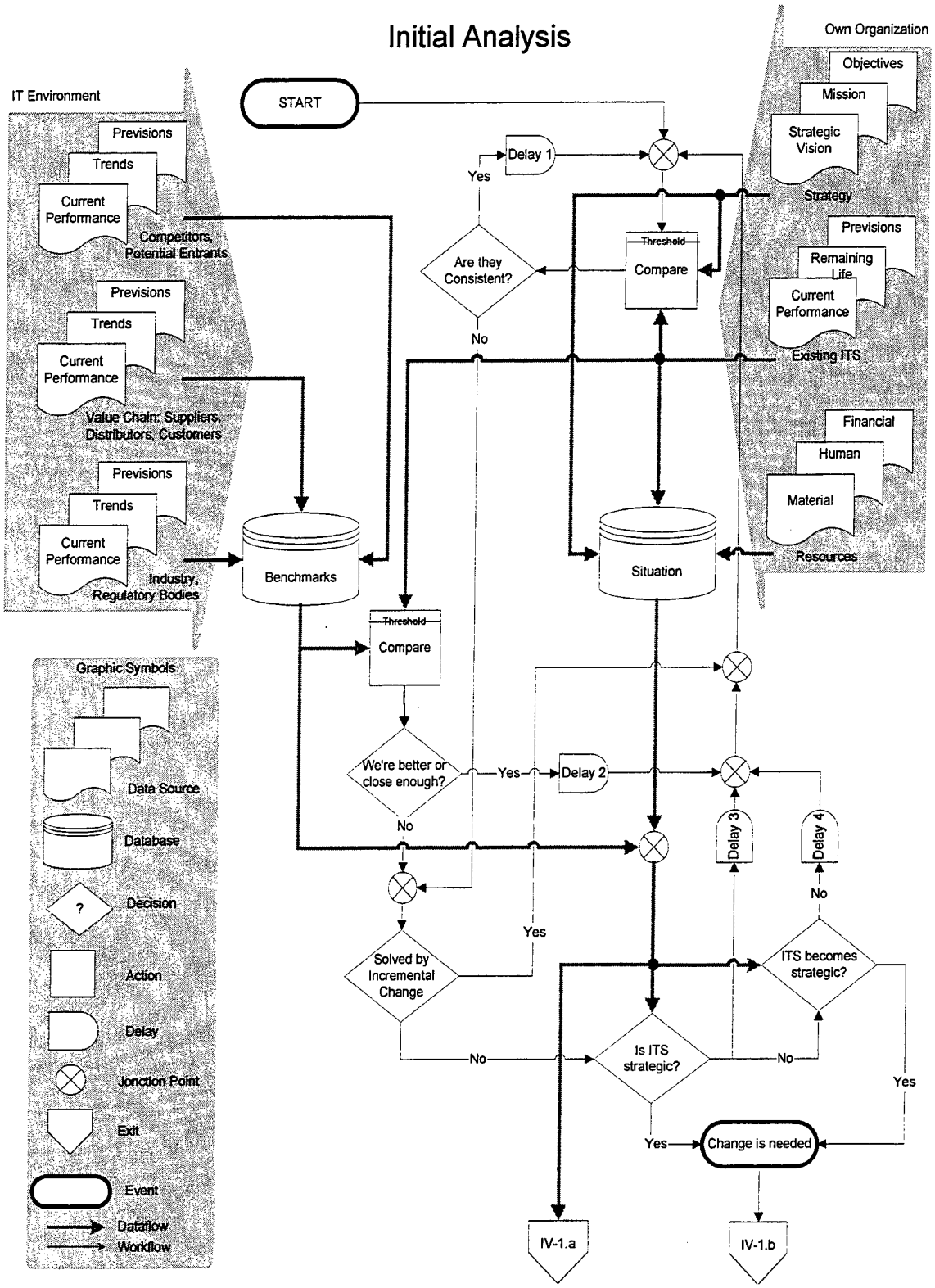
Initial Analysis
IT Environment
Previsions
Trends
Current Performance
Competitors, Potential Entrants
Previsions
Trends
Current Performance
Value Chain: Suppliers, Distributors, Customers
Previsions
Trends
Current Performance
Industry, Regulatory Bodies
START
Delay 1
Yes
Are they Consistent?
No
Threshold
Compare
Own Organization
Objectives
Mission
Strategic Vision
Strategy
Previsions
Remaining Life
Current Performance
Existing ITS
Financial
Human
Material
Resources
Benchmarks
Situation
Threshold
Compare
We're better or close enough?
Yes
Delay 2
No
Delay 3
Delay 4
No
Yes
Solved by Incremental Change
ITS becomes strategic?
No
Is ITS strategic?
No
Yes
Yes
Change is needed
IV-1.a
IV-1.b
Graphic Symbols
Data Source
Database
Decision
Action
Delay
Jonction Point
Exit
Event
Dataflow
Workflow

Figure III-1

Two main sources of information are used in the process: external **IT environment**, and the **organization**. Not all data describing the external environment is relevant for this decision. In fact, the first factor affecting the quality of this decision process is the choice of input data. For example a company producing and selling automobiles needs not, and should not assess its ITS against the one used by a law firm. Similar organizations are more likely to provide a good comparison basis. Therefore, the most important sources of references are **competitors** and **potential entrants**. When the industry includes several market segments with unclear or unstable boundaries and ITS can significantly affect competitive advantage, then it is a good practice to also evaluate own situation against similar organizations present on different market segments, even if they are not direct competitors.

The **value chain** of the product(s) imposes vertical integration for information compatibility. The organization needs to be able to communicate with its suppliers, allies, distributors, and customers — and observe data formats compatibility. A strong bargaining position towards its suppliers and buyers may allow the organization to impose certain standards along the entire value chain. For example, Kodak introduced proprietary formats for digital imaging and succeeded to impose them on both software suppliers and customers (Kodak Digital Learning Center [Ref. 22]). However, this generally is not the rule, and even if it is at a given time, vertical compatibility in information exchange should still remain a concern. As a result of the diminishing life cycle of software products, vertical compatibility became a major driver of change in IT. Because they need to interact with suppliers and customers using prevailing data formats,

organizations are sometimes forced to undergo costly upgrades and migrate to recent versions of the software they use, even if there is no internal need for change.

Industry standards and regulatory bodies' influences on the usage of IT are also factors to be taken into account when weighting the need for change. Proprietary formats may work well for a given period and market segment, but future interdependencies may push for preemptive implementation of more flexible ITS to keep up with the industry standards.

The number and complexity of indicators determines the cost of gathering and process **benchmarking information**. Organizations that try to avoid costs by leaving benchmarking at the discretion of IT specialists set the stage for decisions based on subjective and incomplete information. A set of well chosen and clearly defined indicators for gauging the IT environment constitutes a valuable database and avoids guessing and speculations when it comes to locate the organization in the external context, from this point of view. While identifying relevant indicators and benchmarks is the job of IT specialists of the organization, they also must convey information relevant for the management, so benchmarking should not be seen as an essentially technical task. A dashboard of significant parameters must be agreed upon by both specialists and management, and maintained up-to-date using a clearly defined procedure.

Once indicators are defined and survey procedures set in place, resulting values constitute a database for benchmarking own performances, identifying trends and make forecasts about external developments which may affect the competitive position of the organization.

Internal data used for initial analysis must go beyond the data about the existing ITS and place it against the framework of organizational strategy. A sense of where the organization is heading, what is its main **mission**, and what are its strategic **objectives** (Strickland [Ref. 28]) can put the ITS assessing process on the right track. In addition, a realistic evaluation of the available **resources** helps framing IT projects within the limits of feasibility.

The actual decision process includes five loops and is exited only when a positive determination — stating **change is needed** — has been made. Once change is designed and implemented, the initial assessment procedure starts again and runs until the next need for change is identified.

In the **first step**, existing ITS is assessed against the strategy and resources. If it delivers effective and reliable services, and future evolutions do not display predictable shortcomings, then there is no internal need for change, and **comparison** should be redone after a while (**Delay 1**), to see if things changed. The actual length of this delay is specific to each organization and is determined by the actual role ITS plays in the workflow. Because needs for new or extended IT-based services tend to be identified as work evolves and becomes more specialized, requirements accumulate between assessments and make up a list. Therefore, this first decisional loop must have a predefined **threshold** of significance in order to be able to distinguish between significant needs and fancy wishes. For example, some users could ask for a faster way to access data, while others desire multimedia capabilities on their desktops. A good approach to this issue is to set up beforehand a threshold of significance, allowing to ascertain the merit of each demand against its utility in the work process.

The **second step** is to compare the existing ITS with the external **benchmarks**, and should be performed independently of the first one. If current performance, remaining life and foreseeable evolution situate existing ITS above of or close to the external benchmarks, then no immediate change is needed, and the comparison must be redone after a while (**Delay 2**). Considerations described above about the delay also apply in this loop. However, the significance threshold has a different meaning in this case.

External environment evolves incessantly and keeping up with all new technological developments is neither economic nor technically feasible. Few parameters of IT systems can be enhanced by addition. There are built-in limitations, which cannot be avoided, pertaining to each technology used. For example, the bandwidth of a given network infrastructure, once fully occupied, can only be supplemented by moving to another technology. The result is a continuous change of the relative position the organization occupies in the IT environment. Since internal indicators tend to gradually slip behind external benchmarks, as the gap increases it eventually starts to adversely affect competitiveness and may generate net loss. A solution to this dilemma is to use quantum adjustments, aiming to regain a reasonable position before the gap significantly affects results.

The concept is illustrated in Figure III-2. Consider one parameter used as benchmark, for example LAN throughput (see chapter VII for network metrics). Its value increases in time, as technology evolves. Falling behind the prevailing value only starts to adversely affect organizational results when actual value is smaller than the level labeled "minimum", i.e. when the gap surpasses a given threshold. However, allowing internal level to remain too much behind external benchmark means to incur the risk of crossing

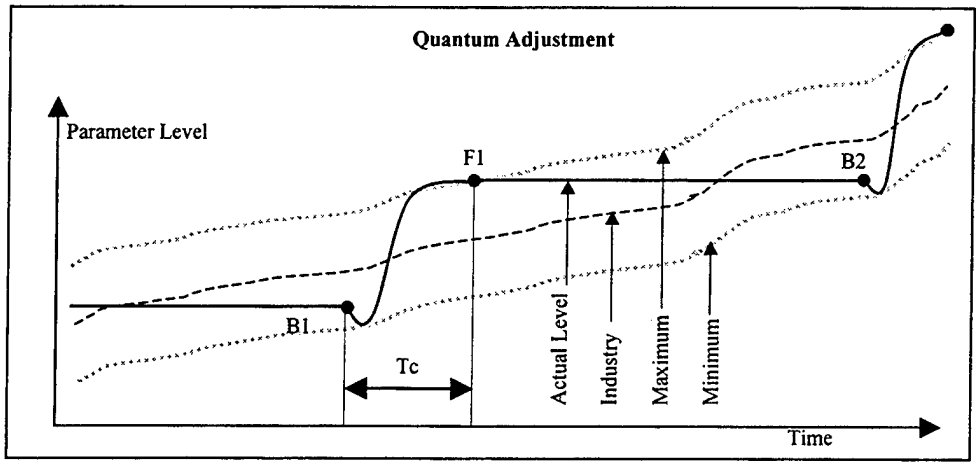

Figure III-2

the minimum threshold during the initial steps of change implementation. Actual change occurs between the begin point (labeled B1) and final point (labeled F1). Because of transitional effects of change, improvement starts to kick in only after an initial fall, when things get worse before getting better. This is due to the cumulative effect of needed alterations in infrastructure and the reflection of learning curve on the overall productivity. Therefore initiating change too late is risky. On the other hand, in order to reap all possible benefits from the existing investment, change should be postponed as much as economically possible. Thus, there is a unique optimal point in time where change must be initiated in order to gain maximum efficiency, and it can only be identified by continually benchmarking.

Up to now, the whole discussion was centered on one parameter, while external environment may need multiple benchmarks to be reasonably characterized, and their respective variations may have different tempos. One solution to this problem uses a combination of management by exception and the weighted average method (Strickland, [Ref. 28]). Firstly, all relevant benchmarks are identified and assigned survey procedures.

Whenever one of them falls toward the minimum level partial measures are initiated to compensate that specific weakness. All values are also assigned significance coefficients, integrated using a weighted average formula, and compared with the benchmark computed by the same rule. When internal result approaches the predetermined optimal point, then it is time to initiate the change.

The third loop in the decision process is entered if either external benchmarking or internal audit surpasses the respective threshold of significance. This step is necessary in order to determine whether **incremental changes** in the existing system can solve the problem. Few IT systems are set up to fully use their capacity from the beginning. Most have limited built-in capabilities for expansion, and incremental upgrades may solve some of the initial shortcomings and postpone the need for a major change. When that is the case, then effects of the available upgrades must be evaluated before they are actually implemented. If detected problems can be solved by incremental upgrade, then the whole process can return to the initial comparisons. However, two more aspects need consideration at this step. First, with older systems, the cost of an incremental increase in performance can surpass the outlays required by a radical change of technology. Second, upgrades seldom add to the overall life span of the existing system. Any of these aspects can justify bypassing available upgrades and go directly for a major change.

The fourth loop in the decision process takes into account the overall importance of ITS for the organization. The question to be asked here is whether shortcomings detected in the previous steps have **strategic effects** on the organization. If the answer is yes, then change is needed, and the initial analysis ends. However, when computers are only used for peripheral tasks and their weaknesses do not affect current competitive

position, investment in a major change is not justified, and the question can be postponed for a while (**Delay 3**). In order to make a decision at this point a simple "quill-pen test" (Haga [Ref. 14]) is sufficient: if ITS would be shut down for a week and the organization could still perform its main tasks without major disturbances, then ITS is not strategic.

If currently ITS is not strategic, but there is a reasonable expectation it will **become strategic** in the foreseeable future, then moving to anticipate projected needs can justify investment in change, regardless of the current situation — case captured by the fifth loop.

Two outputs of this decision flowchart will be used in initiating the next process: the determination to set off the change, and the information about benchmarks and internal situation.

B. SETTING THE TARGET PERFORMANCE

The upper limit for change has more than one possible definition, and several aspects must be considered in order to decide how far should the change go. One approach to this question is technology-based. Limitations imposed by the available technology can be seen as the ultimate, albeit moving, boundary for ITS in any non-IT organization. Beyond this limit is the R&D domain, which exceeds the scope of the present analysis.

When it comes to decide how far the next change should go, specialists argue that the higher the better and the only limitation they accept is the available budget. Two groups of arguments are presented to the management in order to support acquisition of the latest technology: one is based on the accelerated obsolescence affecting IT, and the other builds on future compatibility along the value chain.

The higher we aim now, goes the first argument, the longer we will rely on the solution we implement. Figure III-3 shows how the underlying assumptions work. Implementing now a change from B1 to F1' will move the need for the next change from B2 to B2'. This is a valid conclusion, but is based on several fallacies and its implications should be carefully considered before deciding how high is enough.

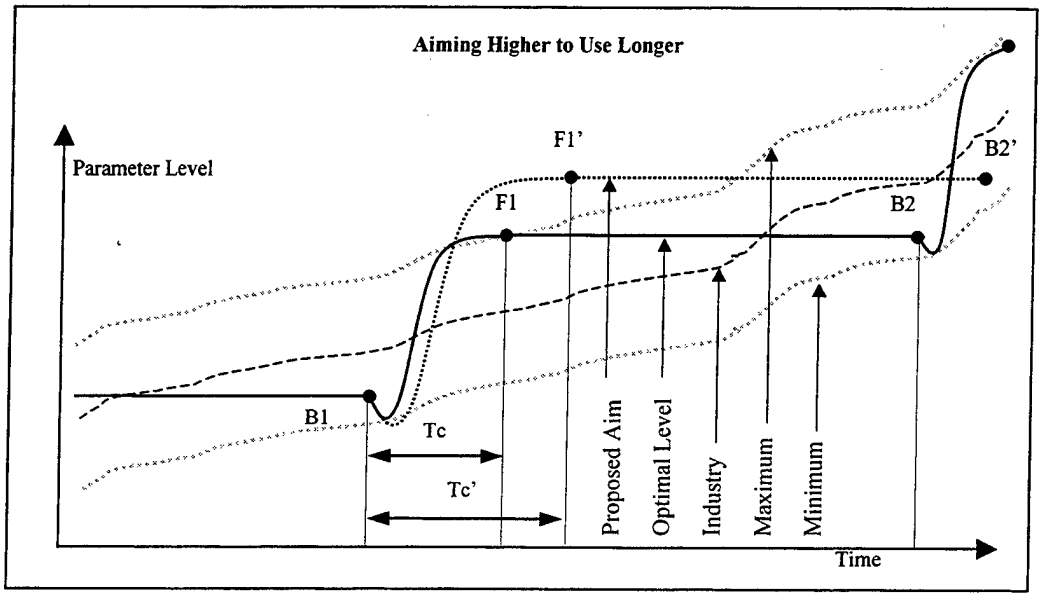

Figure III-3

One aspect is the necessary time for change implementation. Although there is no linear relation between the depth of change and the duration of the process, time is a resource affected by the scope of change (Tc versus Tc') and the longer it takes before the system runs at full capacity, the shorter remaining useful life will be, until the next cycle must be initiated. Thus, a high target, which takes long time to attain, may in fact leave a shorter interval to reap the benefits then a reasonable target level, which takes less time — and also lower costs.

Another aspect is the cost of excellence. As it happens with every domain, higher capabilities come with increasingly higher costs and diminishing returns prevent results from reflecting the level of investment. A technologically attainable goal is not necessarily efficient economically. Moreover, admitting for simplicity that overall costs were linearly dependent of the parameter level (i.e. twice as good IT costs twice as much to implement and operate), then the areas contained between the time axe and the parameter level curves (B1-B2 and B1-B2') are proportional with the overall costs of the two alternatives. Then, for any given time interval, the cost of the upper solution is higher, while the return on investment may be the same.

Another aspect to consider is inertia. Greater investments need longer time to amortize, and long time investments are riskier with IT then with more stable technologies, because of its high rate of change. A flexible approach, providing for frequent adjustments to unexpected developments, can keep the organization closer to external trends and internal needs and avoids sinking resources into initially promising solutions that may lead to nowhere. For example, in the last decade the hardware for system backup increased available capacity by a factor of 1,000, transfer speed by over 200, and added multiple capabilities for automation, while prices for constant performance went rapidly down. In order to take advantage of the new technologies, an organization that would have stacked large tape backup systems only a few years ago would be now in the position to scrap them without ever using their entire capacity, because of maintenance costs which became unacceptable compared to currently available solutions.

Finally, the fallacy that high-end technology always prevents the effects of obsolescence has a built-in contradiction. In fact, technology not only evolves on a non-linear path, but also has unexpected changes in direction. A well known example is the concept of desktop computing, which in the 80's opposed the idea of strong stand-alone computers to a central mainframe. Due to this then new approach, corporate computing environment underwent dramatic changes only to rediscover centralized administration, shared resources and security capabilities that mainframes provided to begin with. It is now obvious that heavy investments in high-end PCs ten years ago did not suffice to keep up with current trends and needs.

IV. SETTING UP THE FRAMEWORK FOR CHANGE

A. DECISION FLOWCHART

Once the initial analysis outlined in the previous chapter resulted in the determination that the IT support is due for a major change, the **first logical step** is to decide how this change will be defined and implemented. Pros and cons for each of the two possible approaches are detailed in the next section. If the bottom-up approach is chosen, then requirements will differ among subsystems and must be processed separately, before the integration phase. This makes the process longer and requires procedures do deal with the specifics of each sub-system. Consider for example the case of a publishing house, which includes two main lines of business, producing respectively forms for governmental use, and high-quality art reproductions, sold as interior decorations to companies in the hospitality industry. Both lines use ITS, but requirements can differ in multiple ways, because forms production is based on large quantities and low graphic quality, while the exact opposite is true for art reproductions. In this case a bottom-up approach can be used to capture, articulate, document and formalize requirements for each line of business.

Regardless of the chosen approach, overall system requirements also need to be processed. In a top-down approach, this is the step where the new ITS is defined, while in a bottom-up approach this phase puts together sub-system requirements and sets guidelines for integration.

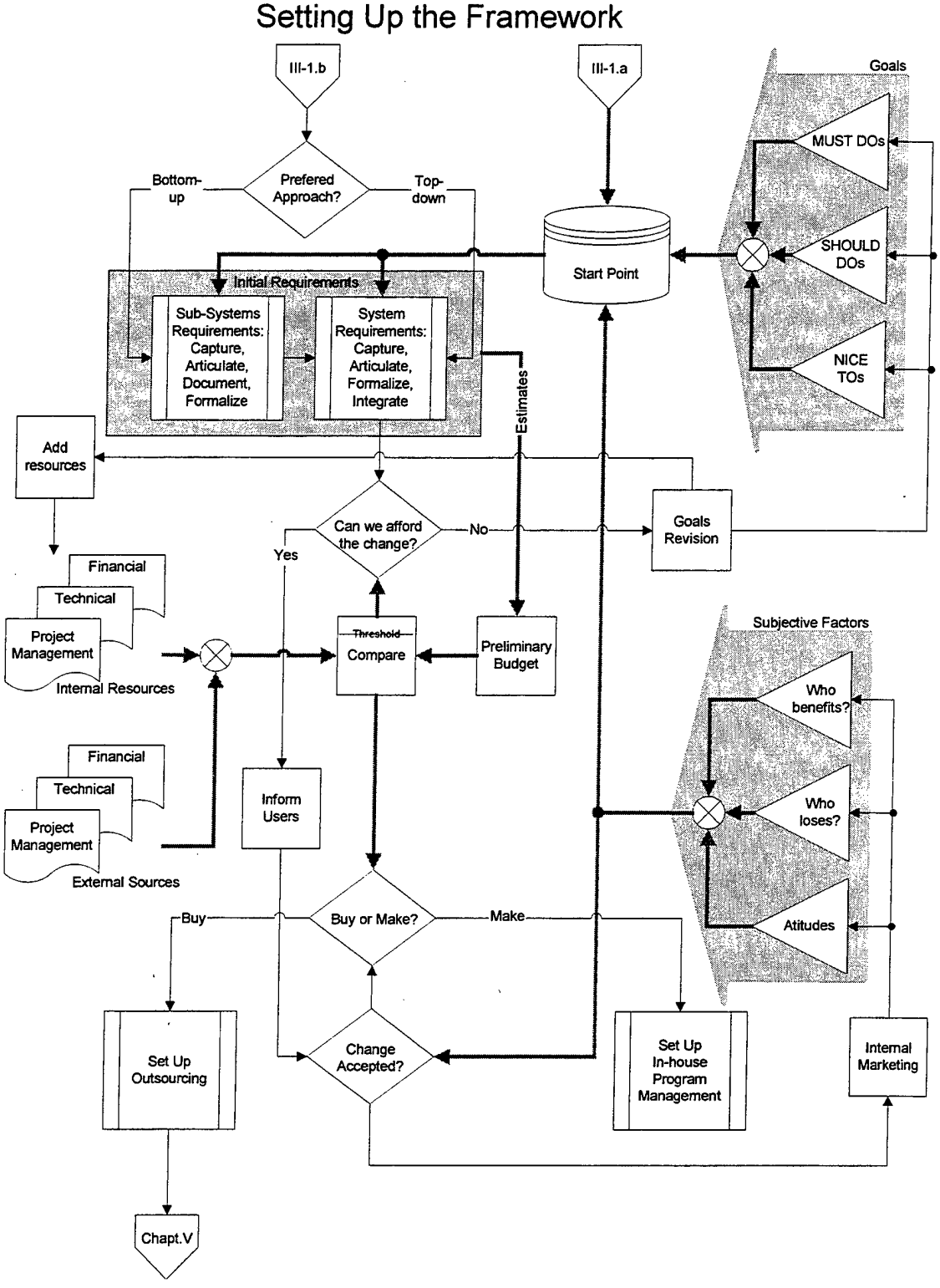
Setting Up the Framework
III-1.b
III-1.a
Goals
MUST DOs
SHOULD DOs
NICE TOs
Bottom-up
Prefered Approach?
Top-down
Start Point
Initial Requirements
Sub-Systems Requirements: Capture, Articulate, Document, Formalize
System Requirements: Capture, Articulate, Formalize, Integrate
Estimates
Add resources
Can we afford the change?
No
Yes
Goals Revision
Financial
Technical
Project Management
Internal Resources
Threshold
Compare
Preliminary Budget
Subjective Factors
Who benefits?
Who loses?
Atitudes
Financial
Technical
Project Management
External Sources
Inform Users
Buy
Buy or Make?
Make
Set Up Outsourcing
Change Accepted?
Set Up In-house Program Management
Internal Marketing
Chapt.V

Figure IV-1

Initial requirements should not identify solutions. The only focus of this phase should be on the needs, both current and forecasted. Therefore three sources of information must be available at the start point: first, data gathered in the initial analysis process from benchmarking and internal audit; second, the goals of change resulted from current shortcomings and forecasted needs; and last, but not least important, internal subjective factors affecting change. Except for the first one, which was discussed in the previous chapter, these sources of information are examined in the last two sections of this chapter. The actual process of turning this information into requirements is described in section C.

Initial requirements offer the overall image of the new ITS, as far as its main functions and needs it should meet. They also can provide a base for initial estimates, based on similarity with existing solutions or built by addition of expected costs per subsystem. The result is a preliminary budget, which puts financial tags on requirements. Not all costs need to be added in a lump sum. In fact, large IT implementations can span over several budgeting cycles, so information contained in the initial budget correlates estimated outlays and financing sources in a time framework.

Because the initial budget is a financial reflection of the requirements, it must be compared with available resources in order to assess the feasibility of the project. Since actual costs are generated by using both internal and external resources, the comparison made at this step should take them all into consideration. A common mistake, which can result in cost overruns, is to omit some of the involved internal resources from this assessment. For example, production space unavailable during ITS implementation, wages of personnel temporarily detached for related tasks or unable to perform their duties during the transition

should be counted as program costs. On the other hand, existing competencies and materials are to be counted as resources and subtracted from the overall cost.

Comparison between the preliminary budget and the available resources needs to use a predefined threshold of significance, in order to allow a margin of error. Both terms of this comparison are estimates and the longer the time horizon, the higher the probability that resulting figures will require corrections. However, an approximation can still be used as base for a decision, and the tolerances included with the threshold can be used later to implement corrections.

The **second logical step**, based on the comparison described above, is to decide whether change is affordable with the identified resources. If the answer is no, then goals must be reconsidered, in order to identify and discard items which may add insignificant capabilities for significant costs. Once this goal revision is completed, only essential features remain to be funded and therefore **adding resources** to cover all bases is completely justified. If supplementary resources are not available, then the whole process is stalled and should only be resumed when it can be supported, which means it should restart from the initial analysis. It is a conceptual mistake to initiate this kind of change without a reasonable expectation of completing it. Also, imposing cuts in requirements in order to fit resources can only yield positive results if expectations are also diminished. It is a common practice to start with a large set of initial requirements, which result in big preliminary budgets curtailed later to fit available resources, and end up with a system which cannot meet unchanged goals.

After having sketched the new system in the requirements resulted from this decisional loop and ensured its financial feasibility, the **next step** is to submit the draft to

those who are supposed to use it. Although some users may have contributed in the process, their understanding of the change is limited to the actual area they were exposed to. Since effectiveness of the new system will be affected, among other factors, by its acceptance, it is a good idea to identify and address problems before they actually appear. Moreover, informing users before plans are implemented can result in early detection of potential errors and encourage personal commitment to the success of the project. Therefore, informative contents and persuasive format must be carefully balanced to help users not only understand the change, but also to buy into the project and get involved in its execution. See section XI.A.2 for a discussion of communication issues.

New technology and modified procedures can induce enough disturbances in the workflow to trigger animosity or even rejection by the users. It is never too early to engineer acceptance, so effective **internal marketing** for the change should be initiated before the project starts. Potential discontentment can be partly alleviated at this point but, more important, features of the projected system can now be adjusted to better fit organizational culture and gain support. This approach imposes attunements along the whole framework cycle covered to date, but potential gains justifies the effort, and the procedure takes less resources than the first time around, because most of the data is already gathered and processed.

The last decision to make before actually proceeding with change implementation is a choice between outsourcing and an in-house program. The thread of change design and implementation work splits here in two: buy or make. In fact, in each of these two ways there is some of the other. An in-house program includes buying products and/or services, and outsourcing does not equate to total disinterest in, or lack of, internal

responsibilities for the process. Moreover, some functions or phases may be outsourced, while others are still solved internally. For example network security in general can be contracted, while keeping encryption in-house, or an in-house implementation program can follow the outsourced audit and design phase. It is the ratio of internal versus external work to be done that differentiates outsourcing from in-house execution. Actual factors to be considered when making this decision are discussed in more detail in chapter V.

Once this last decision is made, one of two steps remains to be done in order to conclude this phase: setting up the procurement or the in-house program management. Although these two actions are mutually exclusive, they share some traits. Both build on the information gathered to-date and both are meant to define and assign responsibilities to actual people in the organization. The outputs in both cases are managerial guidelines for the process about to be initiated and a division of tasks for the involved people and teams.

B. CHOOSING AN APPROACH TO IT ANALYSIS

The choice to be made here is a dichotomy between the top-down and the bottom-up approaches. There is no unique correct solution for this decision, as each option has advantages and disadvantages. However, avoiding to clearly define and articulate an approach to the process does not create a third choice, but sets the stage for conflicting action and inefficient implementation, as valuable information will oscillate between top managers and actual users.

Top-down approach means creating and/or updating the IT structure from the "top" or the "center" and propagating the change towards lower levels. It usually results in centralizing the process, i.e. implementing a unique set of hardware and/or software standards throughout the system. The central authority might initially collect data about

users' needs, opinions and preferences, but there is a unique central point of decision for most policies, whether they regulate major security issues or just wiring solutions. A unique project of the new system is developed, and specificity is discouraged or even outlawed. The first reason for choosing this approach is usually its concordance with the managerial style of the organization, but there are also other reasons supporting it:

- Centralized design and implementation permits standardization of equipment, software, consumables, maintenance, training, procedures, and formats. Therefore, resulting TCO in a relatively homogeneous organization is lower.
- Security policies can be applied uniformly and used at their potential.
- Design costs are lower, because standard sub-structures (both hardware and software) can be reused and duplicated to cover additional functions and/or areas.
- Subsequent changes can be conceived and implemented easier, since most subsystems are standardized. Modifications in standards are reflected in the entire system and their propagation benefits from uniformity.
- Compatibility and interchangeability between subsystems are the norm, and no special efforts are necessary in order to ensure attunement of similar structures.

Bottom-up approach means individual functions or areas in the system are designed implemented separately and then integrated. Regional or functional subsystems can thus respond to specific requirements, without reservations for processes that are particular to other areas. For example, the human resources subsystem in a publishing company has little need for graphic capabilities, while designers cannot work without, but have no use for a powerful personnel database. Creating the two subsystems separately

can offer to users the kind of processing capabilities most fit to the actual work they perform. It does not mean integrating requirements should be let out of picture until the integrating phase. On the contrary, all the common structures must be defined before the actual implementation of subsystems, but can be actually created as sub-systems are added. Supporting arguments for a bottom-up approach draw on the drawbacks of centralization and the advantages of distinctiveness:

- Standardizing does not always result in reduced costs. An organization with significant differences among workplaces as far as required processing power is in fact bound to waste resources, because the standard should be set high enough to satisfy most requirements, while peak demands may go unsatisfied.

- When it comes to security, centralization is a two-edged blade. A highly centralized security system can be extremely strong and efficient but, once breached, the whole organization is defenseless. On the other hand, successive and independent insular layers of security measures are harder to administer but, if combined in such a way as to complement each other, they may be more difficult to breach.

- Specific combinations of hardware and software packages are available to maximize effectiveness for particular tasks: graphic design, multimedia production, assets management, accounting, communications and so on. Implementing functional sub-systems can maximize the return on investment for such specific solutions.

- Collaborative work tends to occur mostly within functional or regional divisions of an organization, based on similar problems and frequent use of the same resources. A bottom-up approach can facilitate diversity and support the natural division

of work into sub-systems, with common pools of data and processing features, and highways of information between sub-systems.

- Although managing global change in a non-standardized IT environment can be difficult, time consuming and costly, local flexibility is higher, because variations in requirements for sub-systems can be easily accommodated without changes in organization-wide standards.

C. TURNING EXPECTATIONS INTO REQUIREMENTS

What actual users perceive in their interaction with ITS are not technical specifications, but the way the system meets their expectations. Strategic organizational goals are also stated in terms that have nothing to do with network parameters or IT benchmarks. However, actual equipment and software must be selected, acquired, installed, configured and assessed using an objective basis, and this is where requirements come into play. Requirements are collections of formal specifications describing significant features the system must provide, with acceptability thresholds attached. Since all user expectations are not significant for the overall performance of ITS, some will not be reflected in the requirements. In order to make this sort of choice, a filtering procedure needs to be set up. Furthermore, selected expectations must undergo two changes to become specifications: formalizing and threshold definition.

1. Sources of Data for Requirements

Specifications included in the requirements can be based on data from one or more of the following sources:

- Laws, regulations and instructions pertaining to the organization;

- Federal Specifications (FEDSpecs) for Government Agencies;
- Departamental Specifications (for example MILSpecs for DoD);
- Purchase Descriptions (PDs) for Government acquisitions not covered by the previous two sources;
- Benchmarks from the external IT environment;
- Industry standards;
- Market survey reports;
- Promotional materials, descriptions, presentations, and samples provided by producers and distributors of hardware, software and IT services.
- Organizational strategy — vision, mission, objectives;
- Users' expectations which are not currently met by the existing ITS;
- Available internal resources (material, human, financial).

External sources offer information on legal or technical constrains, on attainable levels of performance, and suggest functions or needs that may be covered by the new system. In fact, because producers strive not only to meet current needs, but also to anticipate or create new ones, external sources constitute a pressure factor for continuous investment, even when internal needs are well covered by current capabilities.

Internal sources of data rarely present themselves in structures or forms directly usable in defining specifications. Instead, data needs to undergo a specific process to extract and prepare useful information for specification defining. The process is outlined in the remaining of this sub-chapter.

2. Capturing, Articulating and Documenting Expectations

Most users have some idea about their expectations from ITS, but if asked to lay down a clear set of specifications they would stop short for lack of proper terms, or would produce a set of parameters gathered from friends or mass media, hardly related to the actual functions IT is supposed to support in the organization. Although users' satisfaction is among the targets for the new system, expectations can not and should not be allowed to become specifications without proper processing, because fuzzy requirements make a poor base for design and implementation and move decision from this initial phase further into steps where errors come with costs attached. For example, a statement reading "the interface should be user-friendly" inserted into a set of specifications will force designers to implement their own view of this feature, which does not necessarily reflect the original expectations and may subsequently trigger protracted remedies.

Capturing needs and expectations should be a continuous concern, since management, planners and users only voice their requests if there is a reasonable expectation to fulfill them. Various channels can be used for this purpose: periodic surveys, interviews, meetings and so on. Existing ITS can also provide effective and easy to use channels for capturing feedback to be used in profiling the next change: e-mail discussion groups, bulletin boards, feedback forms, customer service databases, suggestion forums and so on.

Articulating expectations in a coherent manner is the first filtering step, which needs to be taken because users' natural language can conceal the real underlying problem. What users describe is the syndrome, i.e. perceivable effects of the problem, not

its causes. For example a data input operator who interacts with a set of online forms may suggest a more compact form design to eliminate scrolling time, while in fact a simple adjustment of screen resolution can solve the problem without resorting to form redesign. Another employee might complain about eye fatigue, without knowing that flickering monitors are the source of this nuisance. Since more causes can generate the same problem and one cause could have multiple effects, this step should not attempt to solve the problems, but the identify possible connections and unify the language used to describe problems. A good practice for this kind of work is to prepare and use a comprehensive and expandable list of shortcomings, pre-classified by IT sub-systems, reported effects, affected departments, time of occurrence and other relevant criteria.

Documenting expectations means putting them into an objective perspective: identify and investigate contexts that produce repetitive errors, trace cause-effect relations and assess consequences. This step also allows improvement suggestions to be evaluated for technical feasibility and costs.

3. Filtering and Formalizing

Filtering expectations is a necessity because the more accessible feedback forums are to users, the more they tend to throw in any idea they might have, regardless of its relevance for the actual work. There is a trade-off to be made here, since restricting users access to feedback procedures means losing potentially significant inputs, while easy feedback threats flooding management with irrelevant data. An effective filtering procedure can solve this dilemma and offer pertinent information for decision-making. While capturing expectations is an administrative task, articulating and documenting

them are technical duties, and filtering requires management involvement in at least two stages: criteria definition and report assessing.

A set of pre-defined criteria is used in this process to evaluate the merit of each expectation before allowing it to become part of the requirements. Since these criteria allow deciding what passes and what will be discarded, management should review and judge each criterion against the policies resulted from strategic intents. For example, a company decided to implement a team-oriented structure in its departments will support proposals conducting to groupware-based ITS and reject requests for extra individual processing power.

Shortcomings of the existing system must be thoroughly investigated and classified, in order to be addressed and solved by the new system. Three groups of goals can result from this analysis: deficiencies that must be solved (the "must do"s), new features that could improve effectiveness or efficiency but are not essential (the "should do"s), and those that users would like to have but are not relevant to the work at hand (the "nice to"s). Distinguishing among the three groups and assigning the proper degree of importance to each goal provides a better base for subsequent trade-offs required in the cost-benefit analysis phase.

Requirements for the new system can not be built exclusively on users' expectations, because they also must reflect organizational strategy, and this is the point where management must directly contribute to the process. Reports summarizing filtered requests and suggestions, together with provisions aimed to enact strategic objectives, make up the general concept of the new system. Although this is not the end of

requirements creation process, at this point all needed information is gathered and clarified, thus the only remaining action is to formalize it.

Formalizing requirements means translating desired features of the new system into quantifiable specifications and attaching acceptability thresholds. At least two thresholds should be defined for each specification: target value and rejection limit. The former is the level of performance aimed by the change. It covers current needs, planned developments and provisions for unexpected events. Let us consider for example the delivery deadline for a new human resource management database. Actual limit for shutting down the old system might be a year from now, but target value for the new implementation should be set to at least six months prior to that moment, to ensure continuity and migration of data. Rejection limit is the worse value of the given specification that can still allow completion of designated tasks. It equates to the target value, minus contingencies. In the example above, admitting data migration could be performed in a month, rejection threshold for the deadline can be set to a month before the old system will be shut down. Failure to meet this threshold means discontinuity of service and may entail costly remedies. It also can trigger penalties or legal actions for reparations, if implementation is outsourced.

4. Types of Specifications

Functional specifications describe deliverables in terms of results to be obtained and intended use. They neither specify a particular approach or solution, nor impose parameters or values specific to a given product. For example, a requirement stating: "users must be provided with shared access to a graphic database" does not impose the underlying OS or the actual procedure for sharing the files. Further clarifications are necessary in the Statement of

Work (SOW), but this type of specification is not restrictive and allows a large selection base. It also places the burden of responsibility for solution identification, selection and implementation on the system integrator, which might be an outside contractor.

Performance specifications describe deliverables in terms of operational characteristics. Although they do not impose a specific approach or solution, they restrict acceptable variants to those ranging within the performance specified. In this case responsibility for the specified value rest with the organization that generated requirements, while the system integrator is only liable for attaining the stated threshold. For example, setting a minimal value for network throughput could cast out all technologies operating under the given threshold. However, the underlying functional goal might be a given transfer speed between users, for a specified set of file types. Let us consider a network technology with maximum throughput below the specified threshold, which can achieve the desired transfer speed by using efficient compression. Under the given performance specification it would be discarded, regardless of its overall cost-performance ratio which might be significantly better.

Design specifications define precise measurements, tolerances, processes, tests and others details identifying the desired product or service. This approach place the entire responsibility for system parameters on the requirements emanating organization, and the system integrator is only constrained to a strict observance of each specification.

Choosing the type of specifications becomes a significant issue in case the program is partly or completely outsourced, because specifications constitute the basis for contractual clauses delimitating responsibilities between contracting parties.

D. COPING WITH THE EXISTING IT

Identifying and coping with technical limitations of existing IT support is usually straightforward. Storage capacity, network throughput, data seeking and retrieving time and so on are easily monitored, benchmarked against industry standards, and assessed in terms of effectiveness. However, once the need for a significant change has been established, steps need to be taken to decide what should be done with the existing IT.

Economic life of both hardware and software is shorter than technical life. As a result, the need for change in IT hits with obsolescence systems which only consumed part of their technical resources. Actual decision should be based on a cost-benefit analysis of existing options. Three choices are available to cope with this problem:

- Sell, donate, or scrap old equipment as it is replaced by the new one. This option eases the implementing of the new system, but the financial benefits are usually negligible, as depreciation of market value for IT is accelerated, following a geometric or even exponential curve, as shown in chapter II. Tax effects of this choice should also be taken into account, in case the old equipment was accounted for by capitalizing its cost instead of expensing it.

- Demote and keep the old equipment in use outside the new system. Demotion refers to the importance of functions assigned to the replaced equipment. This solution does not affect the design of the new system and is recommendable when the benefits of using the existing equipment in secondary functions surpasses potential gains from sale and the tax effects that can be obtained from donating or writing it off. Consider for example an older thin-Ethernet coaxial-cable network using PCs, currently used for collaborative design of printed boards, which is about to be replaced by a new, UTP-

based structured network with UltraSparc workstations. If the old network is in good shape, it can still be used for administrative duties unrelated to the main tasks — like document typing or e-mail.

- Integrate the old equipment with or without upgrade. When the existing equipment and software needs not to be completely replaced and can be used within the new system without significant costs for upgrading and/or integrating, and the remaining technical life ensure enough of a perspective in using it, then it can be counted as a resource already acquired and included in the new design. At least four aspects must be evaluated in this case: 1) the fit between requirements for the new system and the existing IT, 2) position of the existing equipment and software in its lifecycle, 3) direct costs of integration and/or required upgrades, and 4) indirect costs of integration reflected in maintenance, consumables, staffing, administration and security.

E. SUBJECTIVE FACTORS

Regardless of its purpose, ITS must interact with people to perform its tasks. Most systems rely on human input and their output serves to support decision-making or repetitive tasks. This is the case with administrative support, like human resource management systems (HRMS), inventory management systems (IMS), and so on. Some or all of the data gathering process may be automated, especially in process monitoring systems (PMS), but this does not exclude the need for considering reciprocal influences between ITS and the human factor. Consider for example upstream and downstream influences a fully automated computer-based production line could induce in the workflow, or the reaction of the employees to downsizing as a result of automation. At the other end of the process, the output of ITS can alter the decisional process by

generating representations that substitute reality and/or inducing micro-management procedures. These risks are exemplified and discussed in more detail in chapter XI. Assessing subjective factors related to projected change must hence be part of the initial evaluation of costs and benefits, because it permits timely adjustments of requirements in order to cope with foreseeable problems to ensure acceptance and effectiveness.

The new system is bound to alter the way people work in the organization. Thus, the first question to be asked when examining subjective factors is who benefits the change. Some employees might get a more comfortable interface with the kind of data they usually access to perform their jobs, some compartments or divisions might have productivity increased by the new features, and the overall efficiency and/or effectiveness indicators of the work process may be boosted by the new ITS. All these are gains, but only the first is actually perceived as an improvement at the personal level and can trigger favorable reception by the employee. Although abstract benefits can be understood if correctly communicated, when they come bundled with worse work environment they might trigger rejection, while small improvements at personal level can elicit support and lead to success. Not all new features that can bring forth such positive attitudes are expensive, and the satisfaction generated by let's say a natural keyboard on an employee's desktop may surpass the one generated by the promise that the new system will, for example, increase organizational productivity by as much as 5%.

Not all the winners must be within the organization. If current of potential customers, stockholders, creditors, distributors, community members or any other persons may gain from the new implementation it is a good idea to identify and try to maximize their reasons for satisfaction, by including appropriate provisions in the new requirements. Once processed

in this phase, this kind of information constitutes a good base for marketing actions which will advertise and make known the new features to their beneficiaries.

Determining beforehand who loses because of the new implementation may save resources and offer time to address problems as early as the design phase. The first group to be considered at this step is made up by persons closely connected to the existing system. The more radical the projected change, the deeper it will disrupt established procedures. Besides technical determinants, transition length is significantly influenced by the learning curve, which affects all users in various degrees. Some employees may even find themselves unable to adapt to the new system or the need for their positions may be threatened by new or expanded ITS features. A good example of such situation was the move from mainframes to desktop computing, which literally left some IT specialists out of work and forced regular users to learn how to administer their respective computers. Management may also be affected, since migration from a paper-based set of procedures to a more dynamic one, including multimedia teleconferences, online schedules and dozens of messages darting on a crowded screen is not always easy.

External individuals or categories that may be adversely affected by the change must also be identified in this phase. For example, if the new system requires a newer browser to access the e-commerce capabilities the organization could lose all customers that did not migrate to the newer software. Retro-compatibility issues can in fact create multiple problems of this kind, and they must be included in the requirements and addressed. Solutions can range from including special features in the new system to cope with external needs, to keeping some old features still operational in parallel with the new ones, or even offering upgrades to valuable users.

Among the subjective factors potentially affecting the change, some attitudinal aspects and roles are more significant and require consideration:

Champion for the change is an individual within the organization who actively and expressly gets involved in pushing the change along. Although it is an informal role, usually assumed voluntarily, the actual position of this particular person in the organization can make the difference between a successful implementation and a failure. Therefore it is a good idea to identify this attitude and support it with formal, even temporary, authority. The program can thus avoid dual — sometimes conflicting — flows of information and work between the formal project manager and the informal champion.

Another role within the organization, which may significantly affect the outcome of the projected change, is the **guru**. Each organization has one individual whose expertise and experience in IT are recognized — on a real or imaginary base — and sought to solve current IT trivia. That is the expert, the person who has an answer for each question regarding IT and if he/she cannot solve the problem, then the system simply has limitations and needs to be upgraded or changed — at least this is how the word goes. Because of his/hers perceived expertise, informal authority of this person can be considerable and including him/her in the process of change engineering could be more than a good idea — a necessity. The real problem appears when the special status of the guru is not based on real expertise, or the kind of knowledge it is based on is outdated or too partisan for a solution that is unacceptable. In this case the guru should not be included in the team responsible for engineering the change. If the influence he/she may have in the organization is used to create opposition for the new system, then it must be countered before it actually affects the way users react to change.

Inertia affects all organizations that spend enough time and energy implementing, perfecting and using a set of procedures, and ITS is no exception to this rule. People feel threaten by dramatic changes and strive to maintain the work style they know best. Even when known shortcomings of the existing system are eliminated by the new one and actual work environment is more comfortable, they do have to go through training or other adjustments and it sometimes requires modifying long established habits. Because of this phenomenon, when planning implementation time and resources it is a good idea to include contingencies for overcoming inertia, especially for divisions entrenched in stable procedures. New or dynamic organizational structures display in a lesser degree this kind of attitude, thus allowing faster implementation without strong opposition. If the change encompasses subsystems which are significantly different from this point of view and synchronization between them is critical, then inertia must be considered, estimated and addressed. Training and internal marketing are the two main ways to cope with inertia, but employee redistribution can also yield results in this area.

Personal affinities developed over time for certain hardware and software solutions are part of organizational culture. A good example is the difference in attitudes between PC-people, Mac-fans and UNIX-users. Each group argues their preferences are justified and strive to convince the others. An organizational move toward another operating system (OS), even if justified from a technical perspective and founded on sound cost-benefit analysis, may encounter rejection an lead to failure if personal biases of the projected users are not taken into account. The same is true for other components of ITS, like application packages. While specialized, custom designed applications cannot be challenged because they have no equivalent, commercial off the shelf (COTS)

programs usually target a larger audience and compete against similar software products. As a result, rivalries between software products solving the same problems and targeting the same market segments are reflected in people's preferences for a software package or another. Starting as low as e-mail client applications and expanding to complex relational database management systems (RDMBS), the effects of personal affinities are present at every level of complexity, IT specialists being no exception. Therefore management must knowingly ensure a fit between prevalent preferences within the organization and the future ITS solution, or forge a new set of preferences, whichever better fits strategic objectives and is deemed feasible in the given context.

The issue of **whistles and bells** in ITS is about features that only add to users delight, but provide no functional benefits in exchange for the resources they use. Some of these features are requested by the users, while others are part of the hardware and software packages and bought without a real choice. A typical example is Windows OS (all versions) which comes with a long list of futile features, some of them hidden, bundled in the package and sold as a whole (U.S. District Court D.C. [Ref. 7]).

At least four aspects pertaining to this issue deserve managerial consideration: employee comfort, effects on productivity, required resources, and security breaches. **The first** one calls for a simple trade-off between the need to offer a pleasant and comfortable work environment for the employees and the costs associated with this effort. Since features in the whistles and bells category do not add to actual performance, the only positive result is indirect, through user's personal satisfaction. Methods like "willingness to pay" are available and can be applied in order to quantify and assess this effect against its cost. Their actual benefits and limitations are discussed in chapter VI. **The second**

aspect deals with both positive and negative effects such features may have on productivity. Turning work into play can encourage and enhance creativity, but also may undermine concentration, accuracy or precision in workplaces where these factors are key for results. **The third** aspect is about IT resources needed for features in this category, beyond and above those required by functional requirements. Let us examine system requirements for a workstation running Windows 95 OS, used in an administrative LAN for text processing, spreadsheets and e-mail. At a minimum, in order to install and run the operating system and the required applications without optional components, hard drive space, memory, and monitor performances are less than a fourth of the same requirements for a full installation. Moreover, the OS installed without optional components still contains a set of features that cannot be disabled and take up resources, without adding to useful performance. Therefore, the TOC for a system projected to accept and use whistles and bells is bound to be significantly higher, and the choice of using them must be based on sound judgment of their effects. **The last**, but not least significant aspect of this problem is the effect of these secondary features on security, examined in more detail in chapter 9. For now it suffice to point out that supplementary hardware and software required to support whistles and bells add to the complexity of the system, thus affecting its reliability, and open backdoors into the security measures protecting sensitive data.

THIS PAGE INTENTIONALLY LEFT BLANK

V. OUTSOURCING IT ACTIVITIES

A. WHAT CAN BE OUTSOURCED

An organization can outsource anything but its core competencies. In non-IT organizations, all functions provided by ITS can be contracted out, which is not to say that this approach is always desirable or efficient.

Virtually any phase or combination of phases from the IT system lifecycle may be considered for outsourcing, on a project (one-time) basis or as a continuos activity. Some phases, like concept, design, implementation and retirement are discrete processes and can be easier confined into a unique timeframe. On the contrary, administration, operation, security, training, maintenance, current upgrades, periodic audit and performance evaluation, are continuous activities which can also be outsourced, but on a different contractual basis. Segments of major phases can also be outsourced, for example security design, or offer evaluation for acquisition.

Because of the complexity of IT systems, sometimes contractors must gradually pass responsibility for the new system to local administrators and users, thus creating a

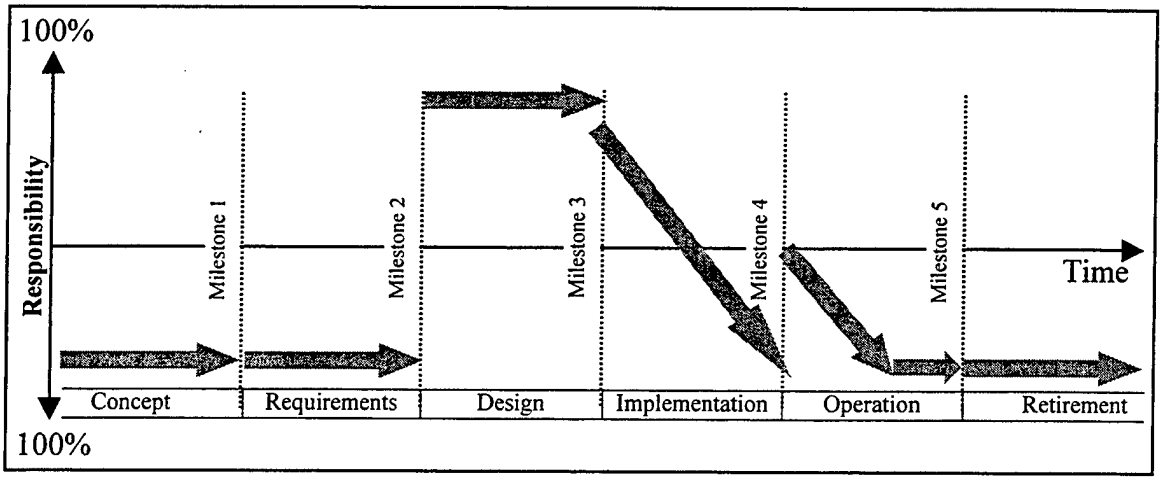

Figure V-1

time dimension for outsourcing. Figure V-2 illustrates this concept.

This example shows an IT system where design, implementation and operation are outsourced, while the two initial phases and retirement are kept in-house. In this case, design falls completely under the responsibility of the contractor, therefore all activities between milestones 2 and 4 are the contractor's concern and do not require participation from the organization. However, implementation is a cooperative phase, and the organization gradually takes over the new system, ending up at milestone 4 with full administrative responsibilities. Because users need to be trained, maybe certified, in order to operate the new system, the initial part of the operation phase is also partly outsourced, with progressive transfer of responsibility to the organization, until a point is reached when contractor contribution is no longer needed and the whole system is fully operational with only internal forces. The last phase, retirement, is solved with internal resources.

Real IT projects can be more complex. Several contractors can perform simultaneously, with or without cooperative tasks involving an arbitrary number of outsourced and in-house operations. Moreover, each phase can be subdivided into activities and each activity outsourced separately or in packages. For example, implementation may include acquisition, building retrofit, power distribution equipment and grounding connections overhaul, network cables installation and testing, servers, hubs, switches, routers and workstations configuring, software installation and testing, web site design, and so on. Each of these activities requires a distinct expertise and may be contracted out or even subcontracted by the main system integrator, which in turn can be a contractor hired by the organization. The same is true for each phase.

Outsourced tasks need not be tied to specific phases or activities from the IT system lifecycle. They can cover specific functions represented in all or some phases, where a particular type of expertise is needed and cannot be covered with in-house resources. Two such functions are good examples of this type of tasks: acceptance tests and security. In order to ensure strict observance of requirements and quality indicators, the organization may choose to retain the services of a third party for acceptance tests pertaining to significant activities in any phase. Since acceptance tests also need to be defined, designed, administered and results reported, quality control can be considered for outsourcing as a whole or by activity. Security is another area where outsourcing can be considered, for any or all activities from the concept to the retirement phase. Because it should be closely customized to organizational specifics and maintain a reasonable degree of internal control, the security function should never be completely outsourced and fits in the category mentioned above, where responsibility is transferred to the organization at a given point, in a more or less gradual manner, at least for core activities like encoding or access rights management. More details about this issue are examined in chapter VIII.

B. REASONS AND OBJECTIVES IN ITS OUTSOURCING

The initial reason for outsourcing IT functions was the explosion of rapidly changing technology and organizations' needs to access new technological benefits at the lowest possible costs. The bottom line was cost containment. Today, things tend to change toward more complex objectives. Although cost containment continues to be a major issue, many companies have other goals as their primary reasons for outsourcing.

The result is a different look in relationships, as companies and their outsourcing vendors push beyond the old parameters to determine ways of achieving new goals together.

Refocusing on core competencies can be such an objective. In 1989, Eastman Kodak was the first company of its size to turn over its computers to an outside organization. It was big news. Consider the fact that on Kodak's manufacturing complex in Rochester, New York, the organization has its own fire house and manned fire trucks. But self-sufficiency comes to a halt when it comes to the business's computer systems. By selling their mainframes to IBM and allowing Big Blue to manage their data processing, it permits the computer professionals to do the computer processing. Before this move, Kodak looked at their computer system as a cost center, with the help of IBM it now looks at information technology as a profit center (Outsourcing Journal [Ref. 23]).

Another example of such objective is investment avoidance. For example, a customer looking at a major capital expenditure for ITS architecture might find a business advantage in pushing the investment to an outsourcing supplier and paying an annual fee for service.

E-commerce also fueled a recent grow in outsourcing, boosting web-hosting businesses predicted to reach $50 billion by 2002 (Albert [Ref. 1]), as companies that have incorporated Internet into their operations realized they need more resources, including expertise, to manage and operate 24 hours a day, seven days a week web storefronts and deal with the thorny security issues involved.

A factor that generates changes over time in outsourcing objectives, is the transfer of know-how that inevitably accompanies outsourced programs in IT. Let us consider the knowledge gained by the internal ITS structure in the example depicted in Figure V-1.

Once they went through the whole implementation process performing their part of the work, they may have gained the capability to do it in the next cycle without help from an external contractor. Hiring specialists or training the existing ones can generate similar effects. The overall result can be **insourcing**, or even **backsourcing**. The first approach is based on accepting ITS internal structure to compete on equal basis with potential contractors, while the second means reclaiming previously outsourced functions or activities. A recent study centered on 14 organizations with two to ten years of experience in IT outsourcing uncovered an emerging trend to pull these functions back in-house as contracts expire or are terminated, and rely more, if not exclusively, on in-house capabilities (Hirschheim [Ref. 15]). Among the reasons suggested by the results were: the newly gained knowledge and know-how, difficulties in contract administration, and a different approach to internal IT, seen as a service provider for the rest of the organization.

When competing against external providers on equal grounds, internal ITS division has at least two major advantages: it doesn't have to add a profit on top of its costs, and can solve sensitive issues — like security — as an insider, without the need for elaborate procedures, set in place to limit contractors' access to confidential information. Moreover, the economies of scale allowing large contractors to benefit from vendor discounts are also available for internal ITS in large organizations, but this advantage tend to become illusory, as small companies get access to discount prices as a result of dynamic technology developments, which rule out price differentiation from the marketing tools of vendors.

In order to choose the actual phases or activities in an IT system lifecycle or the functions which should be up for outsourcing, and to define the terms of the outsourcing contract, three main aspects that need managerial consideration are: 1) in-house capabilities and available resources, 2) benefits and risks associated with outsourcing, and 3) cost estimates and financial arrangements.

In-house **capabilities and resources** need to be compared with project requirements and planned activities in order to identify what can be covered at the required service levels, using internal forces. Not all necessary resources need to be available at this time, but a reasonable timeline for creating or developing required capabilities should be set up and matched with the identified needs. This comparison must take into account material resources — including hardware, software, testing equipment and so on — as well as the human factor and its level of expertise. Because existing capabilities must also ensure continuity of current ITS functions, available resources — time included — must be allocated in a realistic manner between the two assignments before concluding whether they suffice, they must be supplemented, or there is a real need for outsourcing.

Regardless of the existence or lack of sufficient internal resources, before making a decision to outsource one or more phases, functions or activities, the **risks and benefits** associated with the use of contractors need to be assessed in each case. Some of the benefits sought in outsourcing IT are:

- Cost control and containment, attainable by sharing into the of economies of scale obtained by specialized contractors, diminished R&D costs — which are partially

sunk costs for the vendor — and access to wholesale prices through the contractor supply channels.

- Access to know-how and modern technology, without the need to invest and administrate internal R&D capabilities in this non-core area.

- A choice of validated solutions and proven tracks for ITS, thus reducing future uncertainties and allowing planned development.

- Compatibility with other systems upstream or downstream on the value chain, or in the horizontal industry.

- Penetration on new market segments, for example using e-commerce.

- Globalization, using local expertise to deal with both cultural and technological specifics.

- Flexibility in structures and technologies, as a result of a larger basis for solution choices and subsequent modifications.

Here are some of the risks that need to be considered when making an outsourcing decision:

- Cost overruns. The outsourcing contract can cover most cases when actual costs surpass those planned, but this only solves effects, not causes, which are usually beyond the control of the buyer. Also, in a project where terminating the contract and restarting the whole process with a new contractor is deemed more costly than supplementing funds, the contractor can exploit this unbalanced bargaining power and exact for service a higher price than initially planned.

- Communication glitches in transmitting and interpreting requirements and returning feedback. It is important to keep in mind that the contractor shall not do what you want him to do, but what you tell him to do, which may be two different things.

- Job retention problems, with employees in the outsourced services. Even if downsizing is not automatically connected with outsourcing, giving up internal capabilities means a cut not only in costs, but also in expertise, which is not an easy-to-replace asset.

- Security risks. At least two factors make IT outsourcing more susceptible to security risks than other outsourcing arrangements: first, IT deals primarily with organizational information — and the line between public and confidential is not always easy to trace — and second, it covers all or most organizational structures — which makes territorial delimitation impossible or impractical.

- Accountability problems. Limited responsibility is a two-edged principle, which allows setting boundaries to vendors' obligations in an outsourcing relationship, but also leaves room for misinterpretations and litigation. The issue is examined closer in the next section.

- Quality control concerns. Although the basis for outsourcing is trust and confidence in the vendor's capability to deliver expected levels of service, acceptance tests could add to the complexity of project management and create the need for yet another outsourcing contract in order to ensure impartiality and strict adherence to requirements.

- Chain dependencies. Factors adversely affecting the contractor, from small inconveniences like equipment delivery delays, to major problems like strikes or fires will be passed indirectly to the buyer and affect the outsourced functions.

- Reduced flexibility. Paradoxically, outsourcing can narrow the spectrum of available choices, especially when bargaining power is unbalanced toward the vendor and the relationship evolved into dependence for a line of products of services.

- Complex contract administration. IT outsourcing is not a simple procurement, because it intertwines products, services, and organizational information in a unique mix, with effects throughout the whole organization. The larger its scope, the more it departs from the basic principles of acquisition of goods and services and becomes a form of partnership, with new and dynamic rules.

Cost estimates and financial arrangements define the bottom line in outsourcing aimed at financial objectives. However, when other goals are just as important, financial indicators can slide a few notches down on the list of evaluation criteria. Computing cost estimates and assessing the value of financial arrangements in order to create a basis for comparisons could produce misleading results for a number of causes:

- Although hardware and software products have prices that can be added to come up with a total, this may represent only the tip of the iceberg, as design, installation, configuring, customization, and initial administration tasks can represent the bulk of the overall cost, and they differ by large amounts for different solutions.

- The link between increases in performance and the corresponding costs is not linear and sometimes defies any correlation.

- Different producers and vendors use different performance metrics, thus defying direct comparisons and equivalencies and forcing cost evaluations to be based on dissimilar grounds.

- Existing IT which is chosen for integration is carried in the accounting system at values that seldom mirror market value, so new and old equipment are evaluated on different bases.

- Methods used to price IT services differ between vendors, and for the same contractor between activities. For example, maintenance is priced in many agreements on a per-seat, per-month basis, while a package of IT services can use a value pricing method (Everest Group [Ref. 6]).

C. OUTSOURCING CONTRACTS

The management of risk, reflected in compensation arrangements, is the most important aspect that differentiates the types of contracts used in IT outsourcing. Although there is a continuum between contracts that place all the risk on the contractor and the ones leaving it to the organization, a finite number of contract types covers most possible situations (GSA [Ref. 12]):

- Firm Fixed Price contracts.
- Fixed Price contracts with Economic Price Adjustment.
- Fixed Price Award Fee contracts.
- Fixed Price Redeterminable contracts

- Fixed Price Incentive contracts.
- Cost Plus Fixed Fee contracts.
- Cost Plus Incentive Fee contracts.
- Cost Plus Award Fee contracts.
- Cost and Cost Sharing Contracts.
- Time and Materials and Labor Hour contracts.
- Combination of two or more of the above compensation arrangements in the same contract.

Features of these contract types are summarized in appendix XV.A.

Another approach, allowing the outsourcing organization to share both risks and benefits with the vendor is the use of joint ventures as an alternative to traditional outsourcing. For example, Ernst & Young and Farmland Industries formed in 1997 a joint venture to pool resources in IT and avoid the inherent gridlock they saw in traditional outsourcing accountability issues (Trowbridge [Ref. 30]).

Contract types are useful to define a framework for risk management and compensation arrangements, but can not replace meaningful negotiation on actual requirements, levels of service and feedback procedures. It is a mistake to discount the role of negotiations and use "canned contracts", containing standard clauses, offered by some vendors to expedite the process. Because of the close links between ITS and the business processes it support, each outsourcing contract should be considered as a rehearsal of the whole project and customized to closely reflect relevant specifics of the organization and ITS.

According to a recent study (Everest Group [Ref. 6]), most outsourcing relationships created over the last three decades were initiated by companies in financial trouble, and tilted the balance of winnings toward the outsourcer, which used his leverage to impose long contracts with high returns and low flexibility. This situation was reflected in the outsourcing contracts, focused mostly on the technical side and lacking provisions for subsequent improvements in pricing or quality.

Service Levels Agreement (SLA) is the part of outsourcing contracts that defines and quantifies deliverables and establishes performance metrics. SLA includes the view of both contractor and the organization about the ways to implement requirements and assess results. As a result of contract negotiations, initial requirements may suffer modifications, because the vendor comes with another perspective and may suggest enhancements of required features, additional capabilities to cover forecasted needs, or discarding of specifications that only add to the cost or are unfeasible. Besides the negotiated form of requirements, SLA should include the methodology for performance metrics evaluation and the thresholds triggering bonuses, acceptance, penalties, or even contract termination.

In order to avoid future misunderstandings, SLA should clearly define accountability procedures. Strictly technical SLA's offer a poor correlation between the business objectives the organization puts behind requirements and the outsourcer's actual performance against service levels. To reconnect the two and leave as much room as possible for improvement to the contractor, SLA should include metrics that address business issues, not just technical requirements. For example, let us consider an outsourcing contract for hosting an e-commerce web site. Metrics like average processing

time per transaction or up time of the virtual storefront create incentives for the contractor to seek improvements for the underlying technical support and allow subsequent upgrades of technologies used.

The consequences of missing service levels should not constitute overly punitive measures and set the stage for litigation, especially when there are shared responsibilities. Instead they should provide incentives for the outsourcer to take responsibility for the performance and seek ways to add value to the business of the organization. The main steps to be taken when creating service levels are:

- Determine the areas of the organization and the business processes affected by the outsourcing relationship
- Identify and clarify shared responsibilities between internal structures and the service provider. Procedures set to deal with common tasks must cover most possible situations.
- Define metrics to reflect attainment of requirements and business objectives. Adding trend metrics to current indicators can prevent deviations and call for timely adjustments.
- Create mechanisms to connect compensation to service levels attainment.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. COST AND BENEFIT ANALYSIS

A. IT COSTS AND BENEFITS MEASURABILITY

When facing strategic and financial decisions about IT, management of non-IT organizations turns to the same decision-making techniques, tools and instruments they use for other services within the organization. However, IT people often argue that the benefits of ITS defy traditional metrics based on attaching monetary tags to valuate cost efficiency (Hubbard [Ref. 16]). In reality, while some distortive factors may affect the correctness of results, both costs and benefits are as measurable for IT as they are for any other service.

1. Sources of Errors in Cost Computing for IT

Past and current costs for IT are easy to examine if the cost accounting system is set to deal with IT as a separate activity, regardless of the actual organizational structure. A word of caution, though. At least three major causes can distort synthetic conclusions based on accounting figures: 1) modifications in the accounting model, 2) changes in the organizational structure and 3) differences in IT.

Regulations, decisions about depreciation or valuation methods applied, cost allocation techniques, all can change the way ITS — among other activities — is reflected in the accounting system. If this is the case, costs of ITS computed from data recorded before changes occurred need to be adjusted to the current accounting model, before they can be used for forecasts or assessment purposes.

Organizational structure and the way it functions are reflected in the accounting model, which uses specific assumptions, rules and decisions to emulate reality into figures.

Once the original structure changed, the model follows, so comparing cost data for periods in which organizational structure was different can result in misleading conclusions.

Different technologies require differently structured budgets, and IT is quite dynamic in this respect. Therefore, looking at past budgets for guidance on allocating funds for the next major system change or fiscal period could result in comparing apples and oranges and put resources in the wrong place.

Not all cost information must be sought in the organization's accounting system. In fact, pertinent data for future implementations are more likely to be found in external sources, either similar implementations or other public references like specifications, estimates, reports, surveys or studies. Specific solutions adopted in the accounting system to solve problems like expensing versus capitalizing IT investments, materiality thresholds, cost allocation and so on may differ among organizations. Therefore using historical cost data from other organizations without a clear picture of their accounting model may be misleading and should invite caution.

2. Benefits Measurability

Intangible benefits are said to be hard, if not impossible to valuate. Things like data availability, interconnectivity, users' comfort and so on are easily relegated among unmeasurables, but still figure in reports under achievements, sometimes justifying IT budget increases.

A simple mental exercise could help boiling down intangible benefits to measurable parameters[1]:

[1] Adapted after [16].

- If something is better, then it produces desirable, relevant effects. The question here is to identify what exactly are the expected effects if the respective benefit is obtained.

- If it produces effects, then it is observable. Once you know what you are looking for, then you can identify the changes induced by of the intangible benefit.

- If it is observable, then it can be measured. Observable effects can have quantitative indicators attached, i.e. numeric values or intervals to describe variation of effects.

- If it is measurable, then it can be valued. Numeric values can be converted into other numeric values, including monetary indicators, using appropriate conversion formulas and coefficients.

Here is a simple analogy to illustrate this concept of universal measurability: time is an abstraction we use to track succession of events, but there is no way one can see it or measure it. Instead, we use devices that substitute observable effects of time — movement of the clock's arms, flow of sand in a hourglass — for the intangible notion.

After applying this or a similar line of rationing to identify the parameter that has to be measured in order to get relevant information about the intangible benefits, the next step is to choose the appropriate measurement(s). Any indicator or set of indicators can be used, as long as they capture variation of the examined parameter and offer relevant results for the purpose of measurement. For example, if estimation of benefits is part of a decision process aimed to validate an investment in IT, the evaluation indicators can be anything from points to colors or financial ratios. On the contrary, if the goal is to

compare efficiency between IT and other investments, then a more traditional indicator, like the return on investment (ROI) or net present value (NPV) should be computed.

Finally, as in any measurement procedure, the degree of approximation should be taken into account, keeping in mind that numeric results — although they offer the illusion of objectivity — reflect original assumptions and limitations of the measurement method used.

B. OPTIMAL CHOICE: USAGE AND LIMITATIONS

Managerial decisions have two prevalent traits: they are usually made under uncertainty and they attempt to optimize, i.e. to allocate limited resources so as to maximize benefits, or minimize resources allocated to obtain a targeted result. Investment in IT is no exception, but optimizing may become tricky in this case, because of several specific limitations:

- All optimization methods, no matter how sophisticated, are no better than the model used and the input data. Since IT is characterized by a multitude of factors, an attempt to optimize should use multi-factor analysis, which is both complex and unintuitive. Moreover, numeric data describing IT performances is seldom comparable across the board, because manufacturers and distributors use a multitude of parameters, of which few are standardized.

- Statistic data and technical specifications describing IT systems are reactive and particular to the respective solutions. This is to say that apparently similar implementations should be considered with caution before using them for comparisons or forecasts in optimizations for new IT investments.

- Financial indicators like ROI or NPV may offer misleading results if the costs of IT used in computations are affected by the distorting factors described in section A.1. This is to say a solution that seem to offer the highest NPV is not necessarily the best choice in IT, as security issues or quality of the organizational web site (OWS) may be incorrectly reflected in costs.

- Focusing optimizations on IT performances may result in neglecting relevant business objectives. On the other hand, technical performances simply cannot be ignored in this dynamic environment. Therefore setting up an optimization procedure able to provide relevant basis for decision-making involves a trade-off between business and technical variables, and there is no recipe for the right proportion.

- Optimization results are affected by a degree of incertitude, because quantifying all influence factors is neither feasible nor economical. This is particularly true with dynamic factors that shape IT and add volatility to the data describing it. Moreover, although qualitative analysis can provide a working basis for aggregating non-numerical factors into the optimization formula, subjectively valuated parameters can only accumulate into a more subjective result.

C. AVAILABLE METHODS

References in the field use different labels for the methods used in cost analysis. For example, a possible classification looks at the level of complexity and the types of variables used add identifies three groups of methods (Sewell and Marczak [Ref. 26]): 1) cost allocation, 2) cost-effectiveness analysis and 3) cost-benefit analysis.

Cost allocation is a concept grouping methods used to set up budgeting and accounting procedures in order to evaluate the effects of change. The focus in this case is on unit cost or cost per unit of service that allow managers to cope with projects in financial terms of expected results and possible outcomes. This is the basic level for all three cost analysis methodologies, providing techniques for cost measurement, data aggregation, error tracking and levels of confidence for the results.

Cost-effectiveness analysis consists of an optimization that either tries to determine the right proportion and minimal levels of investment for a given goal, or to ascertain the maximum attainable effectiveness for a given budget. Effectiveness is not necessarily estimated in monetary terms, but resources used as inputs variables are valuated in financial terms for comparability. Comparison between applicable projects and variants is an example of specific method belonging to this category.

Cost-benefit analysis goes a step further and looks at the overall economic benefits of the project or program, assessing it against overall required effort, including opportunity costs, in order to evaluate desirability for the intended change.

The actual choice of the methods to be used for an IT project evaluation depends on the depth of change and the resources, including time, available for performing the cost analysis. For example, if you plan to migrate the human resource management (HRM) database from the current DBMS to a new one in order to enhance its capabilities, you could settle for a cost allocation procedure. On the contrary, decisions like switching core operations to e-business need more thorough consideration and could use the higher degree of sophistication provided by cost-effectiveness or cost-benefit analyses.

Performing a cost analysis can pursue three different purposes: 1) ex-ante evaluation, 2) retroactive reporting and 3) intervention modeling.

The first goal means assessing effects of the project before it is actually implemented. In this case the analysis is previsional and can be used to forecast results. A word of caution pertaining to this approach: the resulting prognosis is only as good as the input data and the method used. Moreover, there is always a factor of uncertainty in the result, so predictions should not be taken as infallible. It is a good idea to include with the analysis an evaluation of the degree of certitude, based on statistical variance of the inputs and the tolerance induced by the methods used.

Retroactive reporting looks at programs or segments of programs already implemented in order to identify errors and/or factors of success, to be used for corrective actions or subsequent implementations, or to compare actual results with initial forecasts. Because cost data for past actions is readily available, this type of analysis can be performed with accuracy and may be automated. Considerations exposed in section A.1 about the sources of errors apply in this case and should be taken into account.

Modeling means creating a virtual structure that mirrors relevant traits of the program, linking results with inputs in logical structures, which emulate the anticipated behavior of the original. The procedure is complex and requires sophisticated techniques to capture and formalize relevant throughputs. Once created and validated with experimental data, the model may be used to anticipate the effects of various interventions and provide and figure out the best policies to be applied on the real implementation. Complexity of major IT projects makes comprehensive models unpractical, but segments or separate functions can benefit from this approach. For

example, a reduced-scale model of a large LAN can be used to test and validate security policies or groupware applications.

The steps to be taken in conducting cost analysis for an IT implementation may vary according to the scope and goal of this action, and the allocated resources. The following is a general guideline, to be amended with the particularities of the project:

- Set the scope and the goal for the analysis, including the intended user(s) for results.
- Select relevant data and chose the appropriate methods to process it in order to obtain the expected answers.
- Identify applicable sources of errors and address or aggregate them in order to determine the limits of confidence.
- Gather, validate, sort, prepare and record input data.
- Attach monetary tags to non-financial parameters.
- Apply discounting techniques to account for time value.
- Determine distributional consequences of change: who gains and who loses, and how much.
- Aggregate data and apply chosen analytical methods.
- Conduct sensitivity analysis to point out critical assumptions and available margins.
- Address potential influence factors not included in the analysis.

VII. NETWORKS

"The computer is the network", maintains Sun Microsystems. Modern computing can no longer be based on stand-alone machines, but on networks tailored to reflect organizational needs. We could paraphrase as "the network is the computer", because functions associated with computing now draw on distributed resources and user access information and/or applications located on dozens or hundreds of different machines, located throughout the entire world. Picture this: you need to benchmark your costs for a given product against similar data available to-date. A simple search using one of the gateways available on the Internet can bring on your screen data from hundreds of companies, located on five continents. Simultaneously, the accounting application in your IT system gathers and aggregates internal cost data, and you can compare the results in less than a minute, without delays or written reports. What was the computer you used to solve the problem? Just the one on your desktop? Hardly, since data came from sources outside the local machine, even from beyond your organization. From the network.

A. NETWORK TAXONOMY

In the example above, we already can identify at least two criteria for categorizing networks: 1) location and 2) ownership.

When all components of the network, including servers, workstations, shared peripheral devices and communication media are at the same location, they form a *Local Area Network* (LAN). In most cases, the location can be a single room, a building or a campus. However, existing technologies can extend the distance spanned by a LAN, connecting segments placed at arbitrary locations, even on different continents. The result is called a *bridged LAN*. Although such a network is no longer confined to a local

perimeter, the simple addition of segments maintains the same underlying technology and the outcome is still considered a variety of LAN. appendix B presents the most common LAN technologies.

Initially defined exclusively from a size/location standpoint, the notion of Wide Area Network (WAN) now refers to networks that simultaneously meet three conditions: 1) include subsystems spread over geographical areas larger than a campus, 2) feature scalability to accommodate an arbitrary number of computers at each site, and 3) provide technological capabilities and enough capacity for simultaneous communications between sites (Comer [Ref. 4]).

The real distinction between LANs and WANs actually stems from the technology used to connect the computers in the network. Although LAN technologies can now overcome initial limitations such as the maximum distance between nodes, they were designed to cope with limited numbers of computers, located in the same area. Therefore, the attempts to stretch original capabilities are affected by a diminishing returns effect, and real improvement of performances in large networks requires WAN technologies. Some of the most widespread WAN technologies are also presented in appendix B.

To exemplify the difference and provide a managerial perspective on this problem, suppose you already use LANs for administrative support at central level and two regional headquarters, but they are not connected. The question is how to share information between the three LANs and expand IT support to include local sites reporting to the two regional branches. Three conceptually different approaches can be used to solve the problem: 1) adding workstations for branches and bridging existing

segments into a single LAN, 2) using a WAN technology to connect existing LANs and the branches, and 3) reengineering the entire IT support to form a single corporate WAN. The first solution can only be used if existing LANs are small, and foreseeable computing needs are very limited. The second approach is more effective, and allows gradual implementation. The third is the most rewarding, but also the most costly.

Between the two types of networks discussed above are the Metropolitan Area Networks (MANs), which connect LANs and/or workstations located in a given geographical area, usually the size of a large city, and provide specific services not available in a LAN, in a more economical way than a WAN would do. Such networks are being implemented by innovative techniques, such as running optical fiber through subway tunnels. An example of technology used to create MANs is Switched Multimegabit Data Service (SMDS), developed at Bellcore laboratories in 1995.

A network completely owned and operated by a single organization or an individual is said to be private. Most LANs are private, since they do not include subsystems belonging to third parties. MANs and WANs, however, need to connect remote sites and cross public domain. They also may use long distance communications provided as a service by third parties. Once at least one of the sub-systems included in the network belongs to another organization, then the network is said to be public.

Even if it uses contracted services — provided by a carrier — to interconnect remote sites, an organizational network can still be private if all traffic over public domain is encrypted by the senders and decrypted at the destination, thus limiting to insiders the access to the actual contents of communication. This concept is used to build

virtual private networks (VPNs), which can be implemented on top of any underlying infrastructure and network technology.

Other criteria that can be used to classify and distinguish between networks are:

- Network topology — the general shape of the network. Examples: bus, ring, star, point-to-point. Each topology has advantages and disadvantages and the actual choice should be made after examining them against the requirements and making the appropriate trade-offs between conflicting goals. For example, a bus network needs less wiring than a star, but a cut in the main cable disables it, while the star has no main cable and only one workstation is affected by a cable failure. A topology can be physically implemented using various network technologies.
- Network technology: the actual physical solution used to implement the chosen topology. It includes the protocol used by the network and has specific limitations and features, such as the maximum distance between nodes, type of cable supported, transmission coordination mechanisms and so on. Examples: Ethernet, LocalTalk, Token Ring, WaveLAN, AirLAN, Fiber Distributed Data Interconnect (FDDI), and Asynchronous Transfer Mode (ATM).
- Homogeneity: describes the number of different technologies used in a network. LANs are more likely to use a single technology, so they have high homogeneity. However, mergers or subsequent additions to an organizational network can bring in newer or different technologies, reducing homogeneity and calling for inter-network connectivity solutions. On the contrary, MANs and WANs are inherently non-homogeneous, because they connect remote LANs, which usually differ in many aspects, including networking technology.

B. NETWORK METRICS

Any given network is characterized by multiple parameters. Most of them measure performances and therefore are offered as indicators of quality. However, not all are relevant for managerial decision-making and, more importantly, just a few provide information for comparative evaluation. Two criteria should be sufficient for choosing indicators to compare network performances from a managerial perspective: relevance to the purpose and comparability between individual solutions. The first one refers to the aptitude of the analyzed indicator to reflect the fit between organizational requirements and the capabilities of the system. For example, an indicator showing the level of distortion of audio signal is irrelevant if the organization only transfers text documents over the network, while in a system aimed to handle multimedia teleconferences the same indicator becomes useful. The second criterion allows identification of indicators independent of technical specifics. Financial indicators, like price, TCO and cost of operation and support, meet the comparison criteria. However, they neither report the effectiveness of the respective solution, nor give information on the relative technical performance. Therefore a set of indicators meeting both criteria is required for a clear picture of the proposed system.

A rough classification of the measurements used to characterize network performance could identify the following groups: 1) throughput, 2) response time, 3) availability and 4) reliability.

- **Throughput** indicators show the amount of information flowing on a given path in a given time. Two other terms are used interchangeably, although they are not correct in this context: bandwidth and speed. The former is borrowed from the

communications jargon and its formal meaning defines the difference between the highest and the lowest frequency accepted or generated by a channel or device. The latter is more general and refers to the time taken by a given data transfer unit — usually a packet — to move on a given path. All three notions are interconnected, because broadband circuitry supports high throughputs and high speed. However, what is important to the user is the actual volume of information transferred in a time unit, not the underlying bandwidth or the speed achieved between any two points. Here are the most common values of network throughput:

- 56-kilobit per second: currently the throughput of data circuits used for personal connection to Internet. It requires roughly the bandwidth needed for a voice phone call and is virtually available with any common modem connected to a telephone line.

- T-1 circuit: the minimum throughput useful for an Internet service provider with multiple website clients (1,544,000 bits per second).

- T-3 circuit: the backbone speed of major national Internet service providers (45,000,000 bits per second).

- OC-3 circuit: the backbone throughput that most major Internet service providers adopted since 1997-98 (155,000,000 bits per second).

- OC-48 circuit: the typical speed for many aggregated telephone voice circuits on inter-city fiber optic lines (2,400,000,000 bits per second).

- **Response time** takes into account both hardware and software involved in a specific type of data transaction. It measures the average delay between sending a request and receiving the result. Because each type of request is handled differently by the

system, this kind of indicators is only relevant in the context they are defined. For example, using a response time defined and measured for database query to assess the merit of a network-based teleconference system is irrelevant.

- **Availability** indicators describe access to the services provided by the system. Since networks are essentially shared media, related services are provided according to a rule of precedence, such as First In First Out (FIFO), thus creating an invisible waiting line. If delays induced by the difference between demand and capacity surpass reasonable levels, then the service in question is considered not-accessible and the average availability decreases.

- **Reliability** indicators describe up time or failure rate for the whole system, parts of it, or a given service. Mean time between failures (MTBF), average up time per day, week, month or year, and mean duration of down time are examples of metrics in this class.

A list of the most common network metrics is presented in annex XV.C.

For any given set of metrics used to characterize the networking solution, a number of distinct measurement methodologies may exist. A partial list includes:

- Direct measurement of a performance metric using injected test traffic. Example: measurement of the round-trip delay of an IP packet of a given size over a given route at a given time.

- Projection of a metric from lower-level measurements. Example: given accurate measurements of propagation delay and bandwidth for each step along a path, projection of the complete delay for the path for an IP packet of a given size.

- Estimation of a constituent metric from a set of more aggregated measurements. Example: given accurate measurements of delay for a given one-hop path for IP packets of different sizes, estimation of propagation delay for the link of that one-hop path.

- Estimation of a given metric at one time from a set of related metrics at other times. Example: given an accurate measurement of flow capacity at a past time, together with a set of accurate delay measurements for that past time and the current time, and given a model of flow dynamics, estimate the flow capacity that would be observed at the current time.

One problem with metrics used by various producers, dealers and distributors is their lack of standardization, which makes comparisons difficult and their results unreliable.

Another problem in this area stems from the differences in goals pursued by the proposed measures. For example, let us consider procedures used to evaluate network-based applications Four basic approaches are used to measure and assess application performance: 1) ghost transactions, 2) point-to-point packet inspection, 3) client-based agent measuring and 3) application response measurement. Here's a quick rundown of each:

- Ghost transactions are used by developers or evaluators to mimic activity and record response times, in order to emulate actual transactions for stress testing or capacity planning.

- Point-to-point packet inspection monitors packets as they travel between network points. Although it's an easy way to track applications, there is a drawback: this technique can miss the client side of the equation.

- Client-based agent measuring means equip client workstations and PCs with software agents that clock response times. The advantage to putting a timing device on the client side is seeing performance from the user perspective — a metric IT managers can align with business productivity. This approach also offers a more precise view of query and transaction response times.

- Application response measurement is a set of application program interfaces (API) that reports performance data back to a management application. By using the APIs, an application can leave a trail of its activity and compliant software products can then determine the specific path taken by each request to get a read on response time.

Looking at this example from a managerial perspective we can conclude that choosing a set of metrics is not enough to get a clear picture of the projected performance. There is also a need to ask and understand the standpoint of the measuring technique and select the one that is closest to the specific applications that are being implemented or enhanced.

C. CHOOSING THE APPROPRIATE TOPOLOGY

Network engineers distinguish between physical and logical topology of a network. Consequently, different wiring solutions can be used to implement the same networking technology. Appendix XV.B describes the most common topologies available for both logical and physical structures, outlining specific advantages and shortcomings.

More importantly from a managerial point of view, network topology must emulate and support organizational flows of information, which are usually different from the underlying technical and organizational structures, and have specific features for each organization. To exemplify the differences, the simple organizational chart in Figure VII-1 depicts a hierarchical-functional organization, characterized by the fact that every position reports to a single boss and may have a span of control from zero to a number of subordinates. The arrows show the paths of authority, and there are three layers in the vertical section through this pyramid. Most public organizations and many private ones fit into this model, although the actual details as the height of the structure or the span of control are different for each case.

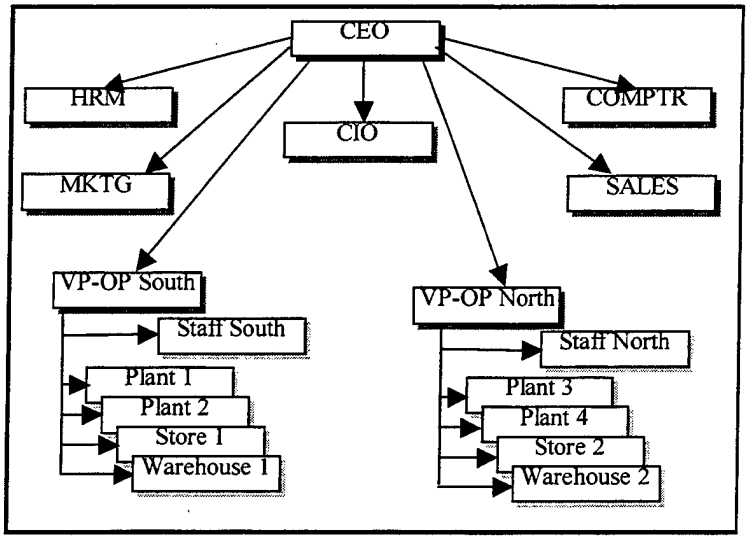

Figure VII-1

However, the flows of information to, from, and inside the organization do not obey the organizational chart, but may display a different pattern, depending on the specific activities they support.

The informational chart for the same organization may look like the one shown in Figure VII-2.

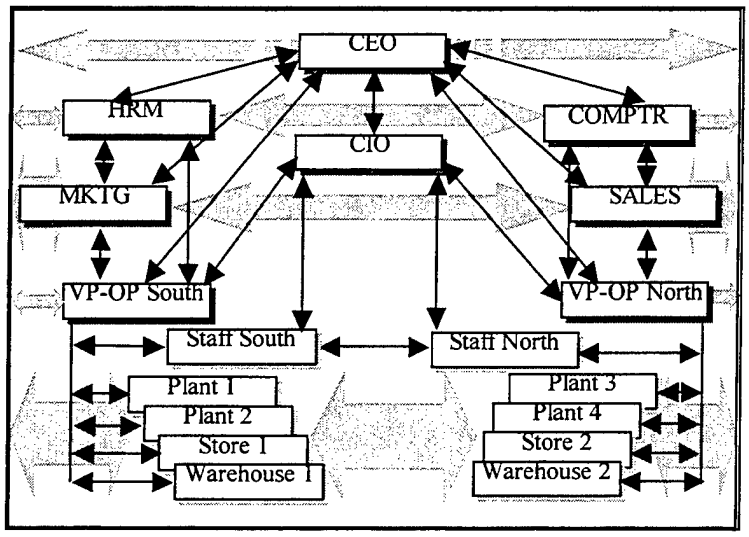

Figure VII-2

The paths of information are more numerous and different compared to those of authority. Divisions and compartments not only communicate among them, inside the organization, but also interact with the external environment. Feedback is added to the vertical channels of command, and information flows both-ways. Quantity of information flowing one way in any given channel is not necessarily equal to the returning one, thus generating unsymmetrical flows of data. Links can be stable over long periods or created *ad hoc,* in order to solve a specific problem. Each channel can transfer printed documents, e-mail, data files, graphics, voice, video, and any information needed for the specific processes unfolding within the organization or with the external environment.

A logical topology apt to satisfy the needs of such an organization is the so-called "bus network" depicted in Figure VII-3. All users are connected to a shared communication medium and the protocols implemented can decide who may connect to

whom, and what data and/or applications are available for each workstation. A unique channel provides all the communications with the outside environment and implements the security policy. The shared medium may include servers for data storage and retrieving, support for office processing, web page, e-mail, groupware, and specific applications.

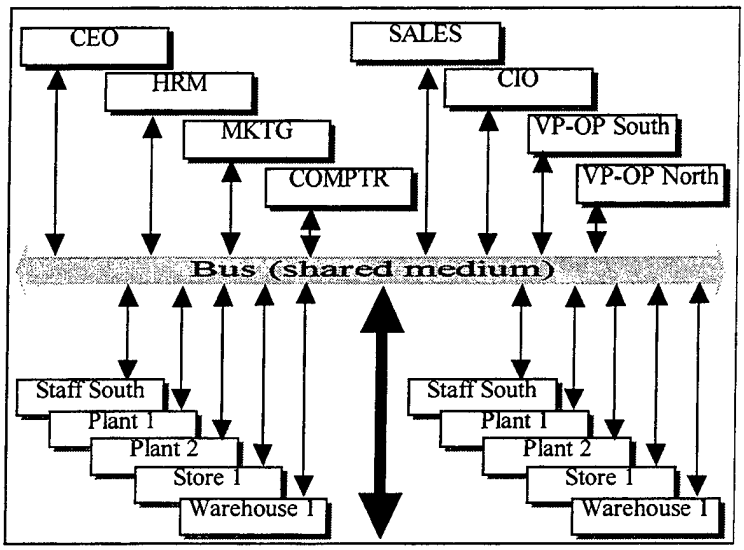

Figure VII-3

All three charts describe the same organization. However, between the hierarchical reports of authority on one hand, and the equalitarian topology of the depicted network there is a difference and an apparent contradiction. In fact, the hierarchy can still be enforced, and the fact that the CEO connects to the network the same way any user does should not be perceived as undermining his/hers position's authority, but as an efficient access to information. Moreover, while a hypothetical network built to exactly emulate the organizational chart may work, it would be affected by delays, unjustified costs, low flexibility, and diminished reliability.

Bus topology is not the only one available. Other solutions such as ring or star may better fit the information flows they support. The important thing to be kept in mind when making the choice is to look at the structure of the information flow chart, not at the organizational chart.

Multiple solutions are available for physically implementing any logical topology, and the actual technology used must deal with the constrains imposed by the building(s) structure, distances between users, quantity and format of data flows, security issues, and existing infrastructure. While the physical design is the sole responsibility of the specialists, the fit between logical topology and data flows can only be achieved as a result of an integrating effort, with users input and managerial coordination.

Funding, however, requires more managerial involvement and a good understanding of short term and long term implications of the decisions taken. State-of-the art solutions are both expansive and risky, because technology may evolve in other directions then predicted. On the other hand, extra capacity can provide enough reserve to expand and develop application originally not included in the project. It is a good idea to look at alternative solutions from the perspective of their future expandability and accept reasonable costs upfront to cover future needs. For example the cabling system, which has a life span surpassing the other components of the network, may meet current requirements with low costs if it uses cheaper solutions, such as UTP cables. Although costs are higher for FTP or fiber-based solutions, over the lifecycle of ten to fifteen years, the extra capacity they provide could save money, because additions to an existing cabling system are more expensive in both direct and indirect costs than initial provisions for expansion. A similar line of reasoning should be used when balancing benefits of

extra throughput against the costs involved. Active network devices also require trade-offs. Fast hubs and switches, with software management features and easy expansion capabilities may stretch the initial investment, but can prove to be valuable assets in the future and add up to smaller TOC for the entire IT system than cheaper but short-lived solutions.

D. DYNAMICS OF THE NETWORK STRUCTURE

Specific structure of the chosen network is a function of its targeted functions and the amount of resources available for implementing the system. On the short term, the most efficient network should closely fit the streams of data required for current information flows within the organization and in connection to the outside environment. However, today's best fit network is apt to be soon affected by obsolescence and overloading, if flexibility is not built-in from the design phase. Consequently, two approaches can be used to tackle future computing needs, avoiding complete reengineering of the system: reservation and expandability. Both solutions are also used by equipment designers, but in a network the right proportion between reservation and expandability is a managerial decision rather than a technical one. This is true first because the network should closely fit the informational model of the organization, which is unique, and second because criticality of the functions to be performed must be weighted against involved costs of performance and compared to the organizational objectives. Simply put, the way the network is set up is influenced by technical specifications of available equipment, but must be decisively shaped to fit the organization. Therefore, the success of a network structure in similar organizations is no guarantee for the same result if specificity is not identified and addressed.

Reservation of extra capacity, set apart for unexpected overloads, increased reliability and future extensions increases the initial cost of the system and generates extra effort for maintenance. Some of the gains from this solution are immediate availability of the reserved resources, technical homogeneity, higher reliability and support for proactive upgrading. Systems using reservation activate supplementary resources as the need arise, but they do not have to implement them after failing to service a number of requests, or suffering repeated overloads. Since reserved resources are implemented together with the main system, technology is the same and does not have to deal with retro-compatibility issues, as in the case of later additions. Some reserved resources, designed to increase reliability, may never be used at all, should the system work flawlessly. However, the cost of losing data, opportunities or valuable time because of equipment failure can be higher than the cost of reservation. Proactive upgrading works well in systems using reservation because increasing demands for service are met continuously by activating reserves, which in turn offer both predictability of extra processing demands, and the time to implement new resources without disrupting the service.

Expandability[1] is the capacity of the system to increase its capabilities by addition, without requiring changes to the existing resources. An expandable system can be implemented with the minimum configuration, which meets current requirements, and grow later to accommodate new or expanding tasks. Costs for implementing and expandable system can be minimal for the given specifications, and upgrades can be

[1] The concept is sometimes referred as "Open System" [11], in order to stress adaptability to evolving environment.

scheduled to meet extended demands. However, unexpected increases in demand cannot be serviced and lead to system overloads. In addition, new or extended functions can only be implemented after the addition of supplementary resources, which takes the necessary time to go through the upgrading process. The need to expand existing capabilities is likely to come when existing equipment is no longer available on the market or its purchase is not economically justified. Consequently, retro-compatibility issues must be also assessed, and this not only includes technical aspects (usually handled by the suppliers), but also maintenance and administration concerns imposed by the increased diversity. Finally, scheduled updates are only as good as the data used in forecasts, but real needs rarely evolve within predictable limits. Therefore disruption of service generated by overloads can occur before the planned upgrade, or business slower than expected may upset scheduled expansions, even if they seemed logical at the time the plan was made.

VIII. SECURITY

First, a few general considerations to keep in mind when coping with ITS security:

- Computer security is an expensive commodity and the results are affected by diminishing return on investment.
- There is no such a thing as an infallible security system, all have potential backdoors, and if they have resisted longer it doesn't necessarily mean they will continue to do so.
- The more complex are the security measures, the more annoying they get to users.
- The more intricate are the security measures, the more inclined are the users to find shortcuts and go around them, rendering them all but futile.
- Building security is a passive action, based on known or imagined ways of attack, while breaching it is active and can be highly creative.
- No matter how strong and comprehensive the security measures are, they are effective only when completely and permanently observed by the whole organization.

A. SECURITY CONCEPTS

A shared understanding of the key concepts used in IT security can expedite requirements generation and avoid misunderstandings, as common words are sometimes used with specific meanings in this context. Here are some of the most important concepts used in IT security:

Identification: the action of correlating an actual user with a user account. The most common identification procedure is based on a username, which is typed, pronounced, scanned or read from another peripheral device.

Authentication: the process of verifying, usually using a password, the identity of a user who went through the identification procedure. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.

Authorization: the process of granting or denying access to specific network resources, based on the user's identity established by identification and verified by authentication, and the specific user rights defined in the Access Control system.

Access Control: mechanisms and policies that define rules to restrict access to computer resources. An access Control List (ACL), for example, specifies what operations different users can perform on specific files and directories. It can be structured by usernames, groups of users, types of files, actions, file locations, and so on.

Data Integrity refers to the validity of data entered, stored, transferred or generated by the system. It can be compromised in any process, therefore measures and procedures need to be set in place to detect and/or correct integrity loss.

Non-repudiation is the principle that prevents participants in network operations to disavow that a particular transaction or activity occurred — a denial that they participated in some activity. It is essential in e-commerce, where contracts are concluded and payments sent directly in electronic form, without traditional written proof of agreement.

B. RISKS AND THEIR SOURCES

The following is a list of security risks that may affect an IT system. The list can be expanded to include specific hazards present in the organization and its environment, or detailed for each category or sub-category into more precisely defined risks. Some risks, like fire or earthquake, are not IT-specific, but need to be considered in the general scope of IT security not only because they can disrupt ITS, but also because they require specific IT protection measures.

Unauthorized break-ins refer to illicit access to system resources. It doesn't necessarily mean people from outside the organization break into the system, since in fact most break-ins come from insiders (Cohen [Ref. 8]) who seek to expand their regular access rights for various reasons. Here are some of the possible purposes and consequences:

- Sensitive Data Leaks: maybe the most common goal of perpetrators — to gain access to data they are not supposed to get into — for malevolent purposes or simple curiosity.

- Financial Fraud: refers to illicit funds redirecting. For example a particular technique, called "slicing" takes small amounts from numerous accounts and redirects them into a target account that ends up accumulating large sums.

- Data Theft: means copying valuable data, like design specifications, chemical formulas or contract negotiation plans in order to sell it to competitors or other interested parties.

- Data Alteration/ Damage: refers to changing or deleting data to hamper its normal usage. It may or may not follow data theft, i.e. damage can be done without prior examination or copying the information.

- Software Damage: means inserting alterations in the normal behavior of some programs, which subsequently alter data they process, without a necessity for the perpetrator to break into the data and change, steal or destroy it. It also can mean disrupting the service the respective software is normally performing, without targeting the data it processes.

- Service Disruption: refers to blocking, slowing down, altering or compromising in any way an IT service.

- Trojans: are small programs masquerading benign or even useful code and mounting attacks from inside the system. Unlike viruses, trojans don't need to hide or multiply, because they are initially accepted as harmful and installed together with normal programs.

- Threats / Embarrassment: refer to break-ins that do not target data or the functionality of the system, but are meant to induce false concerns or to embarrass the organization. Sometimes this type of attack can be used as a diversion, to cover real break-ins or other malevolent actions.

- Eavesdropping/Line Tapping: refer to data interception on communication channels, receiving and decoding secondary electromagnetic radiation or using other procedures to capture information in transit. This type of attack avoids perimeter

protections and focuses instead on weak points along the links between computer systems or between sites.

Screw-Ups: this category of risks groups human or technological errors generated by usage of wrong procedures or correct procedures applied wrongly, without mischievous intentions, but just as harmful as intentional attacks.

- Data Damage: refer to accidental deletion or alteration of data in the IT system.

- Software Damage: means alteration, deletion or usage of wrong settings for the software used in the system. Sensitive software settings made available to untrained and unknowledgeable users can invite wrongdoings and result in serious disruptions of service.

- Hardware Damage: refers to the effects of wrong usage of IT equipment by inexperienced or careless users. Spills, disconnection from network or power, sun or magnetic fields exposures, tampering with systems or peripheral devices, ignorance of standard procedures for storage media use or for refilling paper, ink cartridges, toner and other consumables (if this task falls into users' responsibilities) can all inflict damage to hardware and disrupt functionality.

- Procedures Mix-up: effects of wrong application of procedures for data collection, transmission, processing and storage that do not affect data, software or hardware, but nevertheless produce wrong or useless results and prevent the system or parts of it from performing the assigned tasks. For example sending data to the wrong

recipient or using an inappropriate application for the task at hand doesn't necessarily affect the system or the data, but can generate delays, or financial loss.

Denial of Service (DoS): is a category of risks grouping attacks targeting one or more IT services or their performances, in order to make them virtually unavailable to users. For all known DoS attacks, there are software fixes that system administrators can install to limit the damage caused by the attacks. But fixes can only be effective for the purpose they were created, and hackers are constantly imagining new DoS attacks.

Flood/Pipe Choke: is the most common DoS attack, designed to bring the network to its knees by flooding it with useless traffic, generally by exploiting limitations in the TCP/IP protocol.

Network "smurfing": is a form of DoS generating targeted floods, meant to block a specific workstation or server by emulating ("spoofing") its IP address and broadcasting multiple requests for echoes on the network, thus generating an avalanche of responses sent to the victim.

Viruses: maybe the most mediated form of risk, included here under DoS because of their generic effect of temporary or permanently blocking IT services. They are pieces of code that load onto computers without user knowledge and execute more or less destructive — but always unwanted — operations. Most viruses can replicate themselves. A simple virus that can make a copy of itself over and over again is relatively easy to produce. Even such a simple virus is dangerous because it will quickly use all available memory and bring the system to a halt. An even more dangerous type of virus is one capable of transmitting itself across networks, bypassing security systems.

Physical Damage: defines a class of risks adversely affecting hardware, thus damaging also data and software. It includes, but is not limited to:

- Fires
- Floods
- Power Outages
- Earthquakes
- Equipment Theft
- Vandalism

The terms are self-explanatory, but corresponding measures for prevention and recovery can be complex and costly.

According to the American Society for Industrial Security's 1992 and 1995 studies on industrial espionage, only 40 percent of detected incidents are perpetrated by outsiders acting alone. The other 60 percent of detected incidents involve either an insider acting alone (40 percent) or an insider acting with an outsider (20 percent). Similar results have been published in the Computer Security Institute's study in cooperation with the FBI and in many other studies (Cohen [Ref. 8]). This is different from the common perception that computer security has to deal mainly with malicious hackers and kid geniuses who break into sophisticated protections just for the heck of it. Fact is, intentional breaches originate from, or are initiated by insiders in many cases, and you can add to that all the screw-ups, also produced by insiders. With physical damage from natural or random technological adversities to complete the picture, it becomes apparent that the mediated image of computer security concerns is only a small slice of the real thing.

For each organization and each site covered by ITS, there are generic and specific security risks. It is a good idea to go beyond generic risks and identify what is particular to each site. This effort could save implementation costs for risks that are not present or probable for a given site, and allow customization of protection measures to effectively tackle local specificity.

C. NECESSARY TRADE-OFF: HOW MUCH IS ENOUGH BUT AFFORDABLE?

Successful defenses tend not to rely on a few clever tricks, but on steady long-term effort and constant improvement and adaptation. Therefore, the first thing to keep in mind when implementing computer security is to look at it not as a commodity, but as a dynamic process. Permanent evolution of threats forces security measures to keep up, or even anticipate in a permanent duel between risks and protection. The question to be asked by the managers here is how far do we have to go in order to reap the maximum benefit with minimum overall cost?

One answer to this question looks at the **performance/cost (P/C) ratio**. An example of such analysis is shown in Figure VIII-1.

The chart shows performance and cost values for a number of components (in this case 114 types of data switches) sorted ascending by cost. The P/C ratio has a maximum value for the switch number 18, therefore that is the best buy. At least two underlying assumptions must be true in order to justify such an approach: all the compared solutions must meet the threshold of acceptability, and performance should be evaluated with a unique set of procedures, which is relevant and valid across the board. Now suppose what you need to buy is a security service, and you can choose from a large set of solutions

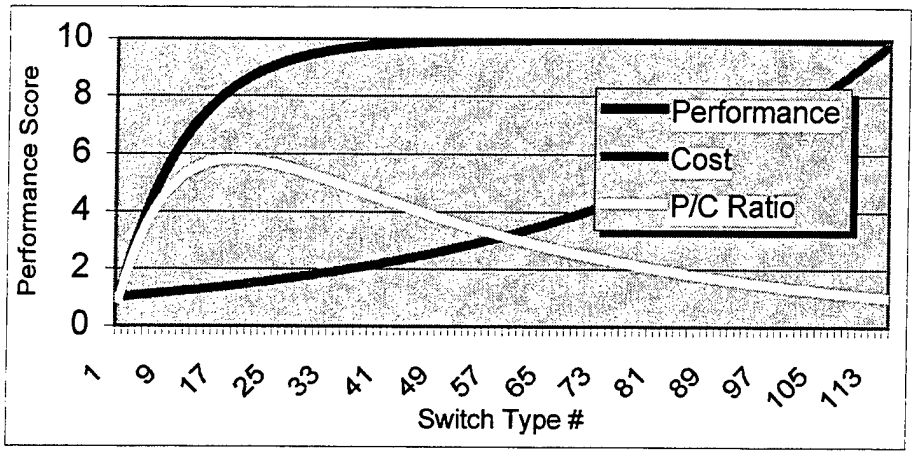

Figure VIII-1

offering different performances for specific costs. This method allows a best-buy choice and one of the terms of the formula — the cost — is usually known, but the result is only as good as the valuation procedure used for assessing performance. Another limitation of this approach comes from its underlying philosophy, based on financial efficiency above all. Computer security is one of the few domains where effectiveness could sometimes dictate against apparent financial efficiency. A mission-critical system, for example, where technical failure can result in loss of human life or serious damages, should be designed and implemented around effectiveness requirements, instead of efficiency.

Other approaches to the problem of how high or how deep security should go are related to the specific strategy that the organization adopts to cope with security issues, may it be a response to expected types of risks, or any combination of the approaches described above.

D. ATTACK AND DEFENSE STRATEGIES

Most human-made security risks are based on motivations and therefore conform to patterns that can be forecasted and acted upon. This is not to say all hackers are

predictable, but covering most such risks is already a major achievement, one that deserves the effort. Here are some of the attacking strategies one could reasonably expect and prepare for[1]:

- Swiftness: meaning hit-and-run, before the victim can detect the attack or react to it.
- Stealth: based on concealment, disguise, and masquerading to remain unseen or to pass for an authorized user.
- Crushing force: usage of flooding traffic or other virtual invasion to overwhelm protection capabilities, or even physical assault on hardware.
- Deception: mimicking other — maybe-benign — problems with the system to cover real attacks or to mislead about the objective targeted, or to test the response.
- Least resistance: mounting strikes on the points considered vulnerable or weakly defended.
- Availability: usage of cracking tools found on the Internet just to try them and gain skills.
- Just as the attackers, who choose the preferred strategy from a set of possible options, defenders can and should make choices of their own when building a mix of security measures. Organizational specifics, results of risk assessment, and available resources — including knowledge, hardware, software, money and time — are influential factors in this decision. Some of the possible strategies that might be considered are:

[1] Adapted after [8].

- Deterrence: aimed to convince potential intruders to go elsewhere by displaying strength and determination to retaliate.
- Deception: intended to either redirect attacks to decoy targets or mimic retaliation without real base to execute it.
- Capture: aimed at luring the attackers into unveiling identification info in order to initiate prosecution or other reparatory actions.
- Adaptive: start with basic capabilities and build reaction capabilities in response to subsequent attacks.
- Preemptive: strike back as soon as the attack is detected, but before it reaches its target.
- Exploitation: making use of the attacker info for the benefit of the defender.
- Cover up: denying attacks and hiding their consequences.
- Variability: permanent change of defense structure and techniques to prevent attackers from finding cracks and using them.
- Overlapping: creating successive layers of different defense measures that cover each other's shortcomings.

The two lists above can be expanded by adding strategies observed in recent attacks or imagining new defenses. Each strategy should then be assessed for the actual conditions in the organization in order to determine its probability and importance. Because managerial decisions in this domain are essentially resource allocations with constrains, it is a good idea to cope with each pair of attack and defense strategies in a decreasing order of significance for the actual situation. For example, each attack strategy can be attributed

a score reflecting its probability, and defense strategies may be evaluated in terms of implementation costs. Then each possible pair will have a probability/cost ratio, which allow sorting the list and coping first with the combinations yielding the highest ratio. Other indicators can be imagined and computed in order to support meaningful choice of the security mix to be implemented.

E. ACCESS CONTROL: WHO CAN DO WHAT, WHERE AND WHEN

All the resources included in an IT system are not necessary to all users in order to fulfill their respective tasks. In fact, if given full access to all resources, users are likely to screw-up the system and make it unusable, even if they don't mean to do so. This means restrictions are not optional, but a necessary part of the security system. The question is to choose relevant restrictions and to implement them in such a way to avoid unnecessary frustrations and protracted procedures. In other words, there is a trade-off between comprehensive restrictions and comfortable work environment.

Three major dimensions should define the space of access rights: 1) the subjects, 2) the objects, and 3) time. It is neither cost-effective nor easy to administer an access control system (ACS) that tries to deal with each user separately, unless the organization has a short payroll. Therefore abstract users — subjects — should be defined and grouped into classes, each class characterized by specific rights. Consider for example a higher education organization. From an IT security perspective all students have similar needs and should be given similar access rights, so the generic subject "student" can be treated by creating a group called "students", with clearly defined restrictions, and managing rights for the whole group, regardless of the number of actual accounts created in that category. Other roles within the organization can benefit from a similar approach,

and actual users can come and go, change positions — thus migrating into another group — or retire, but the abstract subject does not need to be affected by this sort of updates.

Note that this dimension only identifies the who of the ACS, but says nothing about actual resources subjects are allowed to access or other restrictions, like time-based limitations.

The what of the ACS defines actual resources that can be accessed by each group. This succession in access control list (ACL) creation is not compulsory, i.e. ACS can be defined starting from a list of available resources and then building the list of subjects corresponding to each resource. In fact this approach has some merit, as resources may be available on a time-sharing base or restricted by a work schedule. Focusing first on resources allow simultaneous identification of corresponding time restrictions. For example, suppose a printer shared in a network can only be used if consumables are replenished by the person(s) who have this responsibility, and the output needs to be registered, archived, or sent to destinations. If availability of that particular printer is restricted to regular work hours, then attempts to use it beyond that time could produce technical problems, and should be avoided by blocking printing jobs for that period.

Time restrictions can affect both subjects and resources. Therefore, regardless of the preferred approach, the two other dimensions should take time-related problems into account. Availability is not the only time-related issue. Other important restrictions can also be imagined and implemented to block or make difficult impersonation of key personnel by hackers. For example, if a given task can only be performed by two or more users in collaboration, any attempt to initiate work on it at suspicious hours by somebody

claiming the identity of only one of the users should trigger a closer look than usual before access is granted.

There is also at least one secondary dimension of ACS, one that brings it closer to traditional asset security approaches: space restrictions. The equipment composing an IT system is nowadays spread over areas ranging from a single room to global coverage. It can include a number of workstations, servers, switches, routers, cabling structures, communication equipment, data storage devices and peripherals. Normally, all users interact with the system through the workstations and some of the peripheral devices. Therefore all the rest should be out limits to them, accessible only to the system administrator(s). Such kind of protection is not always possible, because of specific conditions and the need to adapt to physical limitations of the building. This creates situations when, for example, network hubs are in the same room with several workstations, printers and so on. Moreover, network cabling structures and communication equipment — for example, a satellite dish — must be mounted in common or open areas. All these and similar situations may require assessing risks and implementing circulation restrictions and physical access measures, which are also part of the ACS.

Physical access rights become more complex with roaming profiles, which allow users to log on and benefit of their access rights from virtually any valid workstation. This makes correlation between physical access limitations and logical measures like identification, authentication and authorization more difficult to implement and more complex to administer.

The final result of access rights analysis is usually an ACL, summarizing who can do what, where and when. It should, by no means, be seen as a dead document to be stuck in a vault and let there until the next major change. Risks evolve, new security technologies emerge, assets are added, updated and removed, and users have a continuous dynamic in, within, and out of the organization, and all these events may require revisions of ACL.

F. PROTECTION MEASURES

A generic list of possible protection measures includes the following:

- Responsible, trustworthy, knowledgeable users, provided with incentives to uphold security policies.
- Pertinent, clearly defined security policies, based on up-to-date risk analyses, backed by at least one contingency plan and administered by well-defined organizational structure(s).
- Periodic back-up and safe storage of important data.
- Access control procedures in place at servers and data storage.
- Controlled and monitoring of user logon procedures.
- Clearly defined, permanent enforcement and monitoring of access rights.
- Effective power back-up system(s).
- Comprehensive database with all hardware and software in use and reserve.
- Mirroring of sensitive data in at least two different sites.
- Encryption of sensitive data and communications.
- Authorizing, scanning for viruses, monitoring and tracking of input data.

- Insurance against natural disasters, fire, theft and fraud.
- Effective and comprehensive maintenance for both hardware and software.
- Authorizing, monitoring and tracking of copies and hard copies generation.
- Controlled and monitored data communications.
- Shielding structures against electronic eavesdropping and line tapping, where appropriate.
- Protection of hardware against unauthorized removal, disconnection, replacement, or tampering.
- Training and coaching of users to develop and maintain security awareness and compliance.
- Relevant system of incentives and disincentives tied to security-related actions.

Not all listed measures apply to any organization, and some specific techniques are not mentioned. However, it is a good idea to list all applicable measures and review it periodically and every time there are reasonable doubts about its current relevance.

G. DATA ENCRYPTION

Encryption means garbling data using a special algorithm in order to make it unusable by others but accessible to the intended user. In order to retrieve the original content, encrypted data must undergo a reversed process, called decryption. The concept is not IT-specific, and was used as early as the Roman Empire, for strategic communications (Network Associates [Ref. 25]). The idea behind encryption is to substitute controlled data alteration for actual data protection, which is harder to

implement and has limitations making it an illusive goal. Before entering a simplified description of encryption used in IT, let us first examine what it can and what it cannot do to enhance security in an IT system.

Users cannot process encrypted data — they only operate with documents written in natural language. Moreover, automated processing, although feasible directly on encrypted data, is extremely time-consuming and requires unreasonable programming efforts. Therefore two major areas pertaining to IT can benefit from encrypting: 1) data storage, and 2) data communication. Assuming all stored data is encrypted, this offers a good protection against data theft, alteration, and damage. It doesn't prevent data loss due to intentional, technological or natural causes. A similar rationing is also valid for communication: encryption prevents or makes extremely difficult eavesdropping / line tapping, but does nothing to avoid data loss or damage. Since financial fraud is essentially based on data theft and/or alteration, encryption emerged as a good solution for e-commerce, where secure transfers are essential.

The problem with symmetric cryptographic systems is the fact that both the sender and the receiver of a message must have the encryption key, so the exchange of keys must precede actual communication. Maybe the most ingenious cryptographic system that solves this problem is based on the public key concept. An important element to the public key system is that the public and private keys are related in such a way that only the public key can be used to encrypt messages and only the corresponding private key can be used to decrypt them. Moreover, it is virtually impossible to deduce the private key if you know the public key.

Public-key systems, such as Pretty Good Privacy (PGP), become popular for transmitting information via the Internet. They are highly secure and relatively simple to use. The only difficulty with public-key systems is that you need to know the recipient's public key to encrypt a message for him or her. What's needed, therefore, is access to a registry of public keys.

Public key cryptography was invented in 1976 by Whitfield Diffie and Martin Hellman. For this reason, it is sometime called Diffie-Hellman encryption. It is also called asymmetric encryption because it uses two keys instead of one key (symmetric encryption).

An example of encryption-based security service is provided by Secure Sockets Layer (SSL), a protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a private key to encrypt data that's transferred over the SSL connection. Both Netscape Navigator and Internet Explorer browsers support SSL, and many web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, web pages that require an SSL connection start with https: instead of http:.

Another protocol for transmitting data securely over the World Wide Web is Secure HTTP (S-HTTP). Whereas SSL creates a secure connection between a client and a server, over which any amount of data can be sent securely, S-HTTP is designed to transmit individual messages securely. SSL and S-HTTP, therefore, can be seen as complementary rather than competing technologies. Both protocols have been approved by the Internet Engineering Task Force (IETF) as a standard (Internet.com Corp. [19]).

H. DECISION FLOWCHART

The first step to be taken when looking at IT security from a managerial perspective is called risk assessment. It starts with **risk identification**, i.e. creation of a comprehensive list of all applicable dangers to your system. Figure VIII-2 contains a generic list, which has to be particularized to reflect actual conditions for the organization. The result goes to the **threat** database, and may also be enhanced by attaching a probability to each risk.

Then actual assets that need protection have to be identified and evaluated. The value attached to each asset may not be equal to the one carried in the accounting system, because it has to reflect what the organization stands to loose in case of a security risk occurrence. Therefore, for each asset on the list there may be several values attached, each one corresponding to a risk that may affect it. The result is a bidimensional matrix, showing costs to the organization for probable risks acting on each asset. Where a particular risk would not affect a given asset, the respective cell holds zero.

There are two approaches to risk valuation: 1) by risk, and 2) by asset. The first one consists of taking every possible risk and identifying the costs of its effects on each asset. The second takes every asset and attach a money value to the effect each risk can produce to it. Both are equally valid and should give similar results. Although the process is simple, because of the sheer volume of work it can take a lot of effort and need high degree of expertise to produce relevant results.

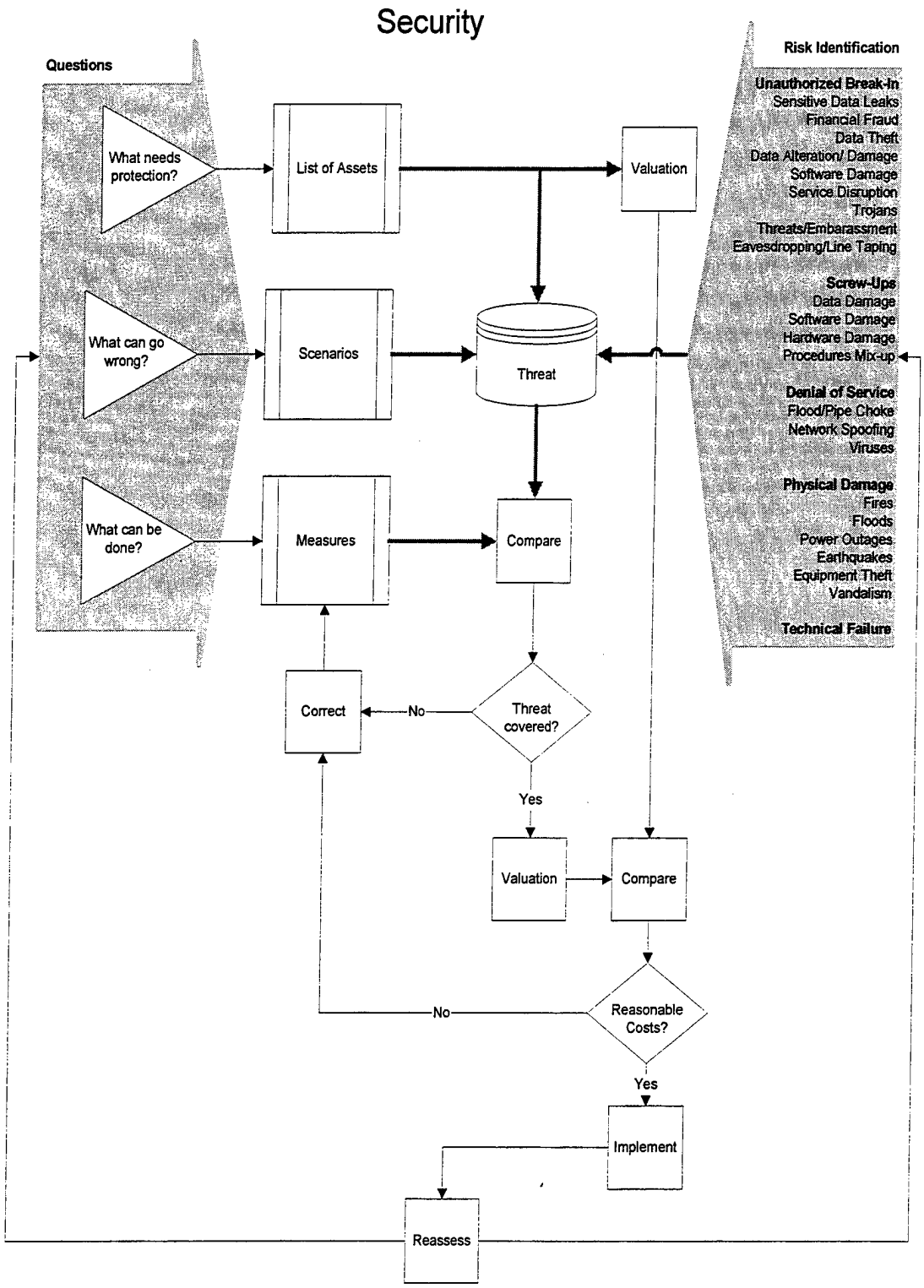

Figure VIII-2

The next question to ask deals with combinations of risks. For example, an earthquake initiating fire, or software damage linked with data alteration, and so on. Plausible scenarios can be imagined and assessed using data from the matrix built at the previous stage. The result is a comprehensive picture of **threats** the IT structure can face in various situations. It says nothing about the ways to prevent or mitigate problems, but can depict their effects in financial terms.

The last question focuses on the existing or accessible resources, grouped into protection **measures** and generating cost evaluations for each such measure. Now the stage is set to make the first **comparison** between threats and measures, which is not a financial evaluation, but a functional assessment of probable results. At this step there is need for a managerial decision, in order to choose the span and depth of desired protection. If essential areas seem to have gone uncovered by the proposed measures, or some specific areas are too weakly defended, then measures can be revised and brought to the desired performances.

The next step deals with financial burden imposed by IT security. This is where some managers make the mistake to compare the overall cost of IT security with a predetermined budget and send designers back to the drawing board to cut wherever function they see fit in order to meet budgetary constrains. A more logical approach is to compare the potential losses computed at the first step, with the costs of protection measures selected. If this kind of comparison gives reasonable results, then budgetary resources should be allocated for implementation. If not, then projected measures can be reviewed to meet constrains. The question here is how to define what is "reasonable".

There is no theoretical answer, as each organization has its own strategy and faces its own challenges, so each manager must define their own threshold of acceptability.

Once IT security is founded and implemented, there are just two things to keep in mind about it: it must be strictly observed, and all the risk assessment process must restart, in order to continuously monitor and evaluate actual inputs, and point out emerging needs for adjustments.

IX. IT AND HUMAN RESOURCES MANAGEMENT

Every major change in ITS is also a good moment to assess the concepts governing the human resources involved. Existing organizational structures, relevant HRM plans, and job descriptions need to be reviewed and projected on the perspective of the new system. Even if there are no technological or procedural reasons for modifications in this area, the knowledge base needed may differ, objectives and intents may have evolved, and there may be previously noted inefficiencies than call for corrections. Some of the issues that need managerial consideration at this stage are discussed in the next sections.

A. IT PEOPLE VS. ALL PERSONNEL

Two approaches are available to manage human resources for IT: hire, train, retain and use specialists, or encourage computer literacy for all personnel. They are not mutually exclusive, as an ITS division can be populated with experts, while the rest of the organization can be brought to a reasonable level of knowledge to use ITS effectively and efficiently. This brings up two concerns for management: organizational structure from IT perspective, and the required level of knowledge for users.

Organizational structure is a product of many factors related to the nature of business and the strategy adopted by the organization. Since ITS is part of it, there must be a fit with other components. For example, in a hierarchical bureaucracy it is more likely to have an ITS division providing service to all other structures, while a team-based organization may integrate different talents, including IT specialists into creative groups working on separate projects. Some of the advantages of having a distinct ITS structure in the organization are:

- Economies of scale. IT expertise is pooled and service provided on a scheduled base, reducing overlaps and time waste.

- Accountability. ITS division can be treated as a profit center and held accountable for both costs and results of the service provided.

- Easy budgeting process. Financial inputs and outputs for ITS are easy to identify, track, plan and manage, using the same methodology applied with any other division.

- Better capabilities to manage major changes, without outsourcing.

- Simple HRM. Selection, training, promotion, and career management can use specific criteria and methodology, benefiting for relative homogeneity of specialties and jobs.

- Effective planning. Current and preventive maintenance, upgrades and back-ups can be planned in order to make the best use of available human and material resources. Using statistic data and a probabilistic model, even interventions for troubleshooting can be planned as far as the kind and volume of resources needed.

- Unified acquisition and distribution procedures for consumables.

- Centralized security administration. This feature can be seen as a disadvantage. See chapter VIII for a discussion of this topic.

- Easy reuse of hardware and software components.

- Standardization of procedures, formats, system settings, and available services.

Not all listed advantages become available in small ITS departments. In fact, there is a certain critical mass that justifies creating or maintaining a distinct ITS department, which depends on the type and size of the organization and the complexity of the needs for this service. Because existence and size of this division must be correlated with the volume, importance and complexity of internal demand for ITS, a comprehensive outsourcing program can even justify disbanding the existing ITS structure.

The alternative to a distinct ITS division is a distributed IT service. Each organizational structure that uses IT can have its own support people to administer resources, execute maintenance, provide assistance, troubleshooting and service. A combination of the two solutions is also applicable. Core IT functions can be performed by a relatively small, specialized compartment, while current duties fall in the responsibility of the non-IT divisions. Although some aspects like accountability and budgeting become more blurry, this approach brings IT people closer to the actual users and let operational and functional divisions customize and manage their own ITS to better meet specific needs. Some sensitive functions, like security, may still remain centralized in principles and methodology, but actual observance of established procedures needs to be delegated to user divisions.

B. SELECTION: KNOWLEDGEABLE VS. TRAINABLE

The second major concern can be summarized in the question of who should know what for the system to run smoothly. The necessary expertise depends on the specifics of the organization and the features of ITS. It can be hired, developed, or borrowed for a fee. The last option means outsourcing, covered in more detail in chapter V, while the ratio between the first two is a decision pertaining to HRM. Setting up the

selection process means in fact implementing this decision, and the main factor that needs consideration at this stage is where to draw the line between the expected knowledge of the candidates and the expertise to be gained later, in the training phase. A high level of required knowledge can speed up integration and add upfront value to the new system. The costs of this approach are both financial — compensation package must be more attractive — and non-financial. Some of the risks in the second category are 1) complex and competitive recruiting, 2) lower flexibility and adaptability to job requirements, and 3) high turnover perspective.

In order to circumvent difficulties in attracting and hiring experts, the organization may choose to shift the focus of recruiting and selection to trainable, rather than knowledgeable candidates. Another reason to prefer this approach can be a custom designed IT system, which requires extensive training anyway. Organizational structure considerations discussed in the previous section can also influence this decision, as job descriptions for IT people in a distributed service structure may call for closer understanding of the business process supported, or even part-time involvement in non-IT tasks. Apart from solving the problems identified above for specialists recruiting, this approach may also offer a larger selection base and the possibility to hire people with skills and knowledge in the specific area of business the organization operates, on top of which IT expertise can be subsequently built by training. Financial resources freed from the lower initial compensation can be transferred to specific training, which, in this case, will require more time and higher investment.

C. TRAINING IT SKILLS

Ubiquity of IT in modern organizations makes computer literacy a necessary part of the basic skills required for most jobs. Since the general educational system provides only a small part of this kind of knowledge, employees without sufficient technical background need to go through subsequent training to cover job requirements. Even people with considerable computer knowledge may need to refocus their skills when changing jobs or the technology they use. The domain is simply to wide and evolves too fast for anybody to be able to acquire enough information during formal education and cover all possible bases.

Organizational training is not an one-time event, but a continuos process that needs to be budgeted, planned, managed and assessed in order to produce the expected results. Because of its technological complexity and dynamic evolution, IT requires constant training just in order to keep expertise up to date. Creating or enhancing computer literacy requires even more effort, because the base that must be covered is larger.

The starting point for any training cycle is to identify, define and measure the appropriate levels of knowledge that best meet current and prospective needs created or about to be created by ITS. The result of this step must be a set of objectives describing the kinds of knowledge and the corresponding levels to be attained. Then the existing base of knowledge must be assessed and compared with the objectives, pointing out uncovered and undercovered areas. A static solution, which solves differences in the short run, is to hire specialists, thus bringing in expertise and balancing needs with capabilities. However, there are costs and risks associated with this solution, and in the

long run the newly acquired expertise will still need to be maintained and enhanced by training, otherwise its value may decline. The dynamic approach to this problem recognizes knowledge is a resource and manages it as such. It takes into account inflows, periodic renewal needs, outflows by retirement and turnover, and puts this information on a time frame to allow planning and budgeting.

Investment in training is not risk-free. People can be reluctant or unable to cope with the new information and organizational effort to offer them access to it may go to waste. They also can feel they are entitled to extra income for knowing more, and get frustrated if they do not get the expected raise. Highly trained employees may become targets for other companies' better salary offers and quit after they just went through comprehensive and expensive training programs. Poor correlation with actual organizational needs may funnel training money toward secondary programs and leave key areas uncovered. The list of possible risks is longer, and it is a good idea to have it sort out for the specifics of the organization and monitored throughout the whole training process.

A thorny problem for managers having to deal with training is to define and use meaningful metrics for monitoring training quality and determine return on investment in this process. While costs are easy to track, goes the argument, benefits escape quantification and indicators can only be built on guessing. There is no unique approach to solve this problem, but the assumption that benefits are not measurable can be challenged with a simple rationing. What if the newly gained skills had to be acquired by outsourcing? There is a cost tag attached to each service, including consulting, computer operation, maintenance or troubleshooting. If ITS enhanced its capabilities or improved

performance as a result of training, then the benefits can be valued using the prices of the new features on the outsourcing market.

Training IT skills is a service that can be performed in-house or outsourced. Although outsourcing training to the equipment producer or vendor is a common practice, before choosing this solution training capabilities of the offeror should be assessed separately, as educational competence and technological expertise do not always go together. The actual choice of the preferred solution should take into account internal resources — both knowledge and training support equipment — and the objectives to attain. Once internal capabilities are assessed and costs estimated, outsourcing could be considered from both effect and cost perspective. It is a good idea to identify and define training programs applicable for each objective, as in-house and outsourced events can be intertwined.

Two alternative modes of IT instruction can be used: 1) conventional classroom or hands-on training with instructor, and 2) self-paced tutorials and software courses, known as Computer-Based Training (CBT) programs, without instructor. The first approach allows students to clarify questions not covered or obscure in the manuals by asking the instructor. It also creates the opportunity for immediate correction of wrong practices and keeps the whole class on the right track by continuous supervision. Because not all users have the same background and the rhythm or knowledge assimilation can differ between individuals, the instructor must align the level and speed of the course to the average capabilities of students. This shortcoming is solved by the second approach, where each student go through the material at his/hers own pace, repeating more difficult steps and adapting the instruction process to the actual needs of information. This is a

good solution for heterogeneous groups of students, eliminates scheduling problems and may be used simultaneously in several different locations. The major disadvantages are lack of interaction with the instructor to ask questions uncovered by CBT materials, poor feedback about instruction progress, and difficulties in planning, because users need different time intervals to go through modules.

D. RETENTION OF IT PROFESSIONALS

Non-IT organizations can find it difficult to retain IT talents for a number of reasons. First, compensation they offer is connected to the profitability of the industry they operate in, and IT industry may be more tempting from this point of view. Second, career track for IT professionals has little, if any incentives to offer in an organization with an unrelated profile. Third, unlike IT companies, where the job itself may be a professional challenge for a specialist in this field, organizations in other industries are not on the technological edge of IT and work is more routine than creativity. Other specific factors can aggravate the problem: remote locations, work environment, strict internal regulations or lack of desired job amenities. On the other side of this relation, aware of their special position in the organization, some IT experts develop specific habits, including relaxed attitudes toward work schedule, request for status and refusal of attached obligations, focus on technicalities rather than business results, and so on. Geographic insularity of IT people can frustrate them, because they need to flock together and exchange ideas, and their need for appreciation require peers appraisal, as they feel non-IT people cannot understand and value their work. Although the Internet can partly alleviate these cravings, it is a good idea to encourage participation in IT exhibitions, fairs, conferences and other forums where they could show their achievements and

acquire both appreciation and knowledge that help them perform their work for the company.

Because of these reasons, coping with the retention issue is not a trivial problem and deserves more than superficial managerial concern, especially when IT has a strategic role in the organization. Here are some ways to solve, or at least alleviate retention problems:

- Use job security as an asset. IT industry is known for volatility and rapid changes are not appealing to all people. If you can offer better job security it might be an attractive amenity.

- Keep the compensation package comparable with IT industry or better. It may be high enough on their priority list to prevent IT experts from leaving in search of better places.

- Use performance metrics pointing out ITS contribution to overall organizational results. See chapter X for a discussion of this topic.

- Create a collaborative work environment. IT people should be involved in decision making and encouraged to see their work as part of the organizational efforts.

- Implement an incentive system tied to business results.

- Make good use of community links.

- Leave gates open for promotion of IT people that have the desire and skills in managerial positions, keeping in mind that effective ITS work means a thorough understanding of the way the organization works and could be a good knowledge basis for managers.

- Cut some slack to creativity, and encourage solutions-seeking with new challenges.

- Involve IT people in training users of the system they administer and getting first-hand feedback from them.

X. PERFORMANCE EVALUATION

Managing IT means maintaining control, but control can only be based on relevant information. As ITS become indispensable to organizations and spending on it increases, managers need reliable means of analyzing, evaluating and improving the results they get for the investment in IT. Specifically, they need to track IT performance in a variety of comparative contexts, relative to:

- original requirements
- internal standards developed by the organization
- competitors
- industry peers
- historical performance
- resources spent in building and/or expanding the system

Organizations need to optimize ITS performance focusing on the effects on the end-users, either direct — if IT is used as an interface with customers, as in e-commerce — or through the products/services offered. In the first case, customers gauge IT quality by comparison with other web sites and other media. Poor performance reflects negatively on the business. Confronted with the issue of evaluating IT performance, managers face a difficult choice among a large number of possible parameters, most of which are inherently technical. Instead of wondering about the meaning and importance of technical metrics, they should ask things like:

- How long does it take to download the e-commerce homepage?
- How long it takes to the system to return a price quote?

- How long does the customer wait before seeing a list of products or services?
- Why does the web site seem slower on one backbone versus another or from one city versus another?
- If current performance is poor, how can we find the source of the problem and improve performance?
- How can we know about performance problems before the customers complain or even before they notice?
- How can we anticipate future problems and adopt a proactive attitude?

In order to set up an effective performance evaluation system, three steps must be undertaken: 1) choosing, defining and managing the appropriate evaluation criteria and metrics, 2) implementing the procedures needed to obtain the metrics and 3) distributing the results to the right levels of decision-making structures.

A. EVALUATION CRITERIA AND METRICS

The overall value of the measurement system is dependent upon the quality of the individual measures. The criteria shown below should be applied to assist the development and evaluation of appropriate measures.

- Relevance: measures should be logically and directly related to organizational goals, strategies and functions and provide a basis for practical decision-making.
- Unequivocallity: measures should provide clear, unambiguous results that leave no room for contradictory interpretations.
- Reliability: measures should produce accurate and verifiable information over time.

- Validity: measures should capture and reflect the information intended, minimizing the influences of secondary factors.

- Coverage: measures should incorporate all significant aspects of organizational ITS.

- Cost-effectiveness: measures should be of sufficient value to justify the cost of gathering, filtering, sorting, processing, storing and distributing the resulting information.

These criteria should be seen as filters and used to block out of the evaluation system metrics that require resources but bring no or low value to the decision processes they are supposed to support. Since decision-making structures and procedures are unique to each organization, the evaluation system must be adjusted to best fit their specific needs of information.

According to their time reference, metrics used for evaluation purposes can be 1) historical, 2) current and 3) predictions. The first group looks at performances for past periods of time and allows comparisons with standards, norms, benchmarks, budgets or planning data. Results are reactive and can only be used for adaptive correction measures. The second group contains metrics for present performance and trends. Results can be used for on-the-fly corrective measures and offer support for a dynamical approach to quality management. The third group builds on the results provided by the first two and creates an image of future results. Good correlation of data used, together with a comprehensive model to aggregate metrics and a dynamic procedure to refresh

information can result in accurate predictions and allow proactive performance management.

Some performance measurement programs fail because the wrong measures are chosen. Others fail because the correct measures are chosen, but the environment changes and the measures do not. Still others fail because senior leaders simply become bored with the measures, and stop paying attention to and reinforcing them (Kelly [Ref. 21]).

The whole evaluation system must work on up-to-date input data. This requirement may become trivial with IT, when gathering, filtering and validating data are automated. However, another aspect may allow obsolescence to creep into the evaluation process if revision procedures are not built-in from the onset: the usage of outdated metrics. In a dynamic environment such as IT, evaluation criteria, metrics used to reflect performance, and measuring methodology evolve continuously. Consequently, a set of metrics that best reflect the status of your system today may become obsolete with tomorrow's technology or business objectives. Therefore, performance measures must be also included in a recurring revision procedure, to make sure they permanently meet the selection criteria outlined at the beginning of this section.

B. SETTING UP EVALUATION PROCEDURES

Once the appropriate set of metrics was selected, the measuring process should be set up in such a way to ensure all chosen measures are based on the pertinent data and the correct methodology, without inadvertently affect the processes they attempt to gauge. Wherever possible, data should be collected naturally as part of the process of work. Measuring processes should not add substantially to the workload of managers, staff, users, or the IT system itself.

Methods used for the chosen metrics should have the property of repeatability: if a method is used multiple times under identical conditions, it should result in consistent measurements. To be more accurate, we could say a method for a given metric exhibits repeatability if, for small variations in conditions, it produces small variations in the resulting measurements.

Some measures and the associated methods are industry standards. For example SPECjvm98 and CPU2000, benchmark suites created by Standard Performance Evaluation Corporation (SPEC) are used for performance evaluation and the results are published on a web page used as reference in procurement (Standard Performance Evaluation Corporation [Ref. 27]). Performance measurements that are specific to certain IT devices or systems are provided by the respective producers. Intel, for example, offers free downloadable methodologies for CPU performance measurements, grouped under three vectors of performance: 1) Integer Performance, 2) Floating-Point Performance and 3) Multimedia Performance (Intel Corporation [Ref. 18]).

Three approaches to IT performance evaluation are available to the organizational management: 1) internal (self-evaluation), 2) external (contracted to third parties) and 3) a combination of the first two.

When sophisticated technical metrics and methods are used, internal evaluation of IT performance is always a self-evaluation, because there is no other structure besides ITS that has the competence to do it. On the contrary, if indicators used for evaluation are business-oriented, they induce comparability with non-IT organizational structures, allow assessments to be conducted from a more objective standpoint — outside ITS — and

encourage stronger bonds between organizational strategy and ITS. Some of the arguments against internal evaluation are:

- Costs of setting up the infrastructure, methodology and procedures for evaluation are entirely borne by the organization and the results may not get benefit from the economies of scale obtained with a professional contractor.

- Quality of the evaluation process internally set up by the non-IT organization may be below the levels attainable by outsourcing.

- Objectivity of evaluation may be affected by the inherent bonds between the evaluator structure and ITS.

- Hardware and software infrastructure used in the evaluation process is part of the organizational ITS, so it is administered and maintained by the structure it is supposed to evaluate, which creates a conflict of interests. In other words, internal ITS has an incentive to tamper with the IT used in the evaluation process, in order to "dress the window" and get credit for performances higher than real.

Outsourcing the evaluation process to specialized third parties can solve the problems listed above, but it also creates other concerns, which have to be considered by managers before choosing the approach that best fit organizational needs:

- Confidentiality of the applications used and data processed by the organizational ITS may narrow down the range of acceptable evaluators.

- Synchronism between organizational strategy on one hand and ITS performance on the other can only assessed by getting a clear understanding of the former

and a good picture of the latter, which means the evaluator must be given full access beyond the actual ITS, to the strategic goals, intents and objectives.

- Specialized evaluators develop and use procedures designed to cover typical organizations. Although they may customize the evaluation to fit the customers' needs and specificity, they rarely deploy the effort of building an assessment process from scratch. As an effect, the results may address only partly the actual phenomena they are supposed to gauge. Instead, reports may offer generic truths and no valuable information for decision-making.

- ITS people may feel threatened when they are forced to undergo external audits. As a result, they could adopt a defensive attitude, and the evaluation may fail to achieve its purpose for lack of cooperation.

C. DISTRIBUTING PERFORMANCE EVALUATION RESULTS

In order to use effectively IT evaluation reports in the decision-making processes, at least three aspects need to be correctly set up: 1) reports structure and contents, 2) where should results go and 3) when should they be delivered. The first aspect refers to the way information is selected, aggregated and presented. The second describes both geographical and organizational locations of the chosen destinations, while the third encompasses time-related concerns.

It is a good idea to organize evaluation reports in layers and create groups of related results within each layer. Conceptually, the reporting structure should look like Figure X-1. Succesive layers get more and more narrow, because raw information is discarded, but use higher degree of aggregation to convey a larger picture of IT.

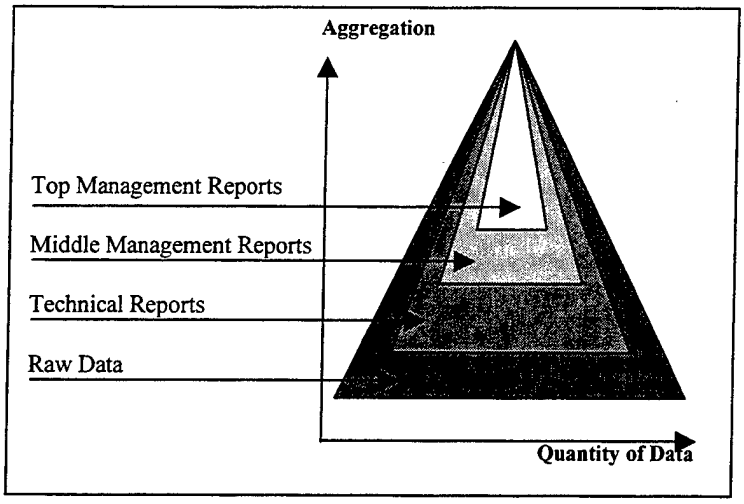

Figure X-1

All raw data collected during the evaluation process reflects the way ITS works, but some of it is simply not relevant, at least in the format it enters the system. Processing methodology must include procedures that allow data aggregation into composite indicators, which trade specificity for generality. Let us compare for example the scope of two indicators: the system's overall response time in a data query and the average track seeking time for a storage device used. Both look at similar notions, but the first one characterizes the system, while the second focuses on a single device. Aggregation is higher in the first case, because the actual value reflects cumulated effects of multiple devices influencing the response time. Not all available indicators can and need to be included with reports for higher echelons, and the selection should meet the criteria outlined in the first section of this chapter. This makes technical reports more comprehensive than the subsequent layers, and sets the higher degree of aggregation for the reports available to the top management. Up to this point we did not mention the actual contents of the reports. In fact, this model can be applied to any of the facets of IT

performance, from technical aspects to budgetary discipline. The raw data basis is different for each type of audit and the triangular reporting structures for various aspects of interest may actually overlap, as illustrated in Figure X-2.

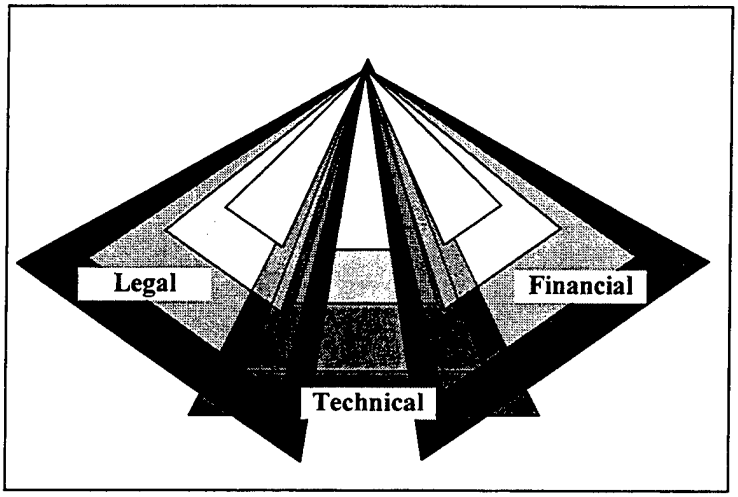

Figure X-2

Overlapping areas are made of aspects simultaneously belonging to two or more reporting perspectives, such as technical, legal, or financial. Consider, for example, the issue of software licensing provisions. Clauses included in the license agreement are both technical and legal, and reports that include references to license administration belong to the overlapping area between the two domains.

The second concern involving results delivery looks at the users of each result to determine what are their informational needs that should be addressed by the reports they receive. Jamming irrelevant information into evaluation reports creates overloading and the significant results get overlooked. On the other hand, excessive filtering and aggregation squeezes out specificity and makes reports look like textbooks valid for any ITS in any organization. A good approach to this problem is to correlate delivered results with the decisional actions they support. For example, circulating a detailed report on the

technical virtues of the newly installed firewall through the comptroller's office will only waste work time and office resources, while data on financial gains resulting from the respective implementation may help the same department in funds planning. Similar reasoning can be applied for geographically separated structures, in order to deliver the right information at the right spot.

Dynamics of IT make time a valuable resource. For example, sudden performance depreciation of the e-commerce site, caused by either technical failure or human error requires immediate corrective action and this can only be done if the reporting system sets the appropriate alarm off. Three types of performance measurements can be distinguished from a time perspective: 1) recurrent, 2) event-driven and 3) by request.

Recurrent performance measurements are performed on a regular basis, using automated data acquisition devices and methods, and can offer a dashboard of indicators reflecting the current status of ITS. If data is stored in historical series it can constitute the basis for statistic processing and predictions. Some information in this category is gathered, filtered, processed and used by the operating system, monitoring software or applications used in IT resources administration. Periodic audits can go beyond this level and include financial, legal or organizational aspects in their scope.

Event-driven performance measurements are executed in order to locate and eliminate dysfunctions, document the needs for change, fundament comparisons, or for benchmarking against various references. Depth, comprehensiveness and scope of evaluations performed in this category are determined by the needs they are supposed to address and the event that triggered them.

Evaluations performed on ITS by request can range from storage media scanning procedures contained in current maintenance and/or resource administration, to comprehensive system audits included, for example, in organizational merger or acquisition procedures.

THIS PAGE INTENTIONALLY LEFT BLANK

XI. TRANSFORMATIONAL DIMENSIONS OF IT

Specialists look at IT from the perspective of its performances. They focus on making it faster, stronger, more reliable and easier to use. Their efforts push the technology forward and as new solutions emerge, the challenges they seek evolve and expand. The managerial perspective on this continuous process has to be open to innovation, and identify the best ways technology can enhance organizational capabilities and improve its competitive position. However, looking at technological dynamic changes uniquely through the filter of a static organization and trying to fit new IT solutions to existing structures and procedures sets back the possible benefits of change and may create dysfunctions, because examined or not, the influence of technology on the organization exists and has its own intrinsic mechanisms. The effects of IT on the organization can be divided into two major areas of concern: 1) structure and process transformation and 2) people transformation.

A. STRUCTURE AND PROCESS TRANSFORMATION

Regardless of the organizational structure designed to implement ITS — whether it is distinct or distributed — particularities of the underlying technology are bound to affect the number of employees needed, their qualifications, and the way the structure itself interacts with other segments of the organization. Let us consider, for example, the transition from a mainframe-based ITS to a client-server architecture. Once part of the processing process migrated from the previous fully centralized structure to the users' desktops, procedures and compartments applying them had to be reshaped to conform to new requirements and tasks.

1. Factors of Influence

The **first** problem requiring managerial consideration at this point is a choice between two possible approaches to creating the fit between technological and organizational structures. In other words, management has to decide whether they want an IT system tailored to emulate current organizational structures, or they are ready to rebuild organizational structures in order to take advantage of new IT capabilities. If change only enhances performances of the existing ITS, but brings only minor modifications in procedures, then the existing organizational structures don't need to be affected. For example, migration to a different operating system for the servers or introduction of an new DBMS are major technological changes for ITS, but users can continue to perform their tasks without even noticing the difference. On the contrary, a move from unconnected desktops to groupware / collaborative applications may dramatically affect the way current tasks are accomplished and require reconsidering some or all organizational structures.

The question to be asked here in order to cope with this decision is how critical is ITS for the organization. If the organization's mission is to produce or deliver a set of goods or services which does not include ITS as part of the technology used, then ITS should emulate organizational structures build around the core processes. For example, in a company in the mining industry which uses ITS for administrative purposes, the production divisions will not reflect in their organizational structure changes in ITS. At the opposite end of the spectrum are organizations built around a process dealing exclusively with information. Let us consider for example a recruiting or headhunter agency. Their core business is to gather, select, sort and sell information connecting other

companies to the labor market. Therefore ITS is their core technology, and major changes in IT should be reflected in the organizational structure.

The **second** aspect connecting IT and organizational structures is outsourcing. One of the main benefits of outsourcing is the fact that it shifts technological concerns from the organization to the contractor. The organization doesn't have to worry about the way technology changes affect organizational structures of the contractor, as long as the contracted services are provided within the agreed clauses. Therefore, the more functions are outsourced, the less internal structures are affected by changes in IT. However, there is a limit to this discharge. Contracts based on per-workplace, time-based fees do not provide incentives to the contractor to optimize the way the organization uses IT services. On the contrary, since the total fee depends on the number and usage of workstations, there is an incentive for the contractor to seek quantity instead of efficiency. Therefore internal optimization is still needed, and outsourcing should not be seen as a panacea.

The **third** aspect pertaining to this relation is the implementation and operational concept behind the new IT system. Building new capabilities by addition means a lesser change, compared to complete reengineering. The first method means existing structures are to be preserved, and the organization moves to newly implemented functions on a smoother path. On the contrary, process reengineering is disruptive and radical, which leads to organizational restructuring. The larger the scope of this endeavor, the deeper its consequences on the organizational chart and the procedures used.

The **fourth** aspect to be considered here is the scope of change. IT systems are organized in layers. The base of the whole edifice is the hardware. Between this level and the users there are several layers, which in turn can be imagined as containing their own

strata. At the broader level of classification one can identify at least six major software layers: communication protocols, operating system, security applications, system administration, software environment, and user applications. All the user sees is the last layer. The system can undergo a complete revamping of the hidden layers without affecting user procedures. At the other end of the continuum, a simple switch to a completely different user interface may impose significant changes in procedures and organizational structures using it. Let us consider for example a warehouse using ITS for inventory management. Migrating the software environment from Paradox DBMS to Oracle RDBMS without any other changes could leave all the procedures intact. However, introducing laser scanning devices for data input could require reconsideration of the whole operation and completely new procedures.

2. Communication and Information Flows

ITS is the plumbing system that carries information throughout the organization. Its structure, capacity and features can help or hinder information flows, can create unconventional channels, modify — or disable — the existing ones, and affect the content of the messages it carries. Although initial analysis identifies the needs for communication and the system is subsequently designed to fulfill them, the influence works both ways, i.e. once in place IT has an active role in shaping organizational communications.

Information flows topology is the first aspect that gets changed by IT. Conventional channels — paper-based data flows, telephone links, fax lines and so on — all represent parallel links that compete with ITS for users' choice. With the advent of multimedia network capabilities, IT added to its already present document interchange

features and covered services previously reserved for other types of media. Moreover, ubiquity of IT capabilities tend to make digital communications availability as common as telephone services, but much more powerful and versatile. This puts the organization looking toward new ITS in the position to restructure both internal and external communications, in order to take advantage of the new features. Consider for example the profound impact that e-mail had on most bureaucracies. A similar thing is about to happen with audio and video digital communications, which allow gaping global distances and creating virtual workplaces irrespective of geographical locations.

Traditional managerial view of organizational information flows used to identify vertical and horizontal channels and combined them in an informational chart, which was not necessarily similar to the organizational one but nevertheless had a pretty clear structure. Topology of an IT-based communication network looks different. Collaborative work and shared resource access added a dynamic dimension to communication and offered support for more frequent stove pipes usage, bypassing hierarchies and conventional gateways. This is not to say IT eliminates pyramids in information channels, but makes them fluid and more project-based than traditional media.

Phenomena such as **overflow, flood, and channel saturation** have different meanings in an IT environment. All refer to volumes of information that are larger than the respective channel can normally support. Given the much larger limits of IT channels from this point of view, the overflow problem tends to migrate to the recipients. Hundreds of e-mails per day may not be a problem for the IT system, but it certainly is for the user that receives them. Moreover, some problems from this category may be

generated by IT-specific causes. The already common notion of "spam" — the e-mail version of "junk mail" — refers to a common phenomenon that exemplifies this sort of problems.

Another aspect connected to the "pipe choke" problem is the need for redundancy. Traditional information flows may have limited capacity, but they are more difficult to disrupt by hackers, viruses, or software bugs. It may be tempting to migrate all information infrastructure to modern digital technology, but keep in mind that reliability is inversely proportional with complexity, and prepare contingency plans to cover informational needs if IT security risks materialize.

Unlike most traditional communication channels, those supported by IT are **virtual**, not physical. This means they not only offer the possibility to interconnect any two or more users on a channel, but also to configure the channel "on the fly", i.e. to allocate resources as needed and reallocate them to other channels when freed. Moreover, data flows optimization can be done dynamically, which means channels are not hard wired and can use specialized software to avoid bottlenecks. Between any two points in a communication network there is a critical path, connecting them on the shortest, cheapest, or fastest way. IT structures can direct messages using algorithms to compute such tracts. Finally, sophisticated filtering capabilities are offered to users of IT-based communications cope with messages — e.g. sort, reject, store, point out, block, and so on — by sender, contents, origin, time and so on. All these features, and more, are available to the organization through ITS, and their usage may expedite or improve communications, but they also induce modifications in habits and procedures.

IT is a pervasive modifier of media choice in organizational communication. People that used to write a memo per month and preferred the telephone or face-to-face meetings to sort-out problems moved to one dozen e-mails per day, each structured like a memo, and gave up meetings considered now a waste of time. Videoconferences cut travelling budgets and made daily or weekly virtual meetings routine. These are but two examples of changes induced by IT in media choice habits. The argument in these cases is availability. In other situations, speed, reliability, or preferred formats can determine the choice, but the migration toward the new media occurs in all cases.

B. PEOPLE TRANSFORMATION

Some of the transformations described in the previous section affect people, as well as organizational structures and procedures. There are also influences of IT that are not reflected in the formal sides of the organization, but reshape attitudes and personal style of managers and employees. It is a good idea to identify and encourage the positive transformations, but keeping an eye on the negative changes could save future efforts to correct them.

1. IT Effects on Management

This group of negative transformations are generated by lack or poor understanding of IT limitations and wrong usage of the newly gained capabilities. At least three errors are common at this level: 1) micro-management, 2) hyper-organizing, and 3) objectivity fallacy.

Micro-management is the temptation of going deeper, to make or at least influence decisions that normally belong to subordinate people and structures. This is not an IT-generated managerial error, but ITS exacerbates it by offering instruments to access

raw information and to involve managers in solving problems at lower levels than they should. This is disruptive in at least two ways: 1) subordinates' own capabilities are not used and 2) the respective managers neglect their own level of responsibility, to poorly cover lower levels.

Hyper-organizing is another attitudinal problem managers might be tempted by IT to adopt. It means implementing a mechanistic bureaucratic approach to most tasks, based on multiple electronic forms, reports, and milestones. ITS can provide enough information traffic capacity to allow gathering and funneling up all sorts of status data that are not necessarily all relevant. Electronic scheduling and planning are easy to implement using ITS, but keep in mind that creativity and sometimes productivity can suffer if work is too rigidly organized and supervised. The capability to do it must be filtered through the wisdom to select only the useful features.

Objectivity fallacy makes managers consider representations as good, or even better, for decision-making process as the underlying reality. They sometimes forget data has to undergo a set of processing procedures to end-up in the reports they read, and somewhere along the line significance may have been shifted from essential aspects to trifles, or essential information may have been filtered out. This is not to say synthetic information based on reality is always deceptive, but assuming a report is accurate just because it was computer-generated can lead to wrong decisions. Even if no processing errors occurred, and all the data presented is accurate, remember automatic validation, filtering sorting and integrating capabilities are only as good as the criteria they are programmed to use, so essential data may be discarded as outliars or obvious conclusions ignored.

2. IT Effects on Employees

Aversion towards objectivity and ubiquity of IT can seriously hinder its effectiveness. Employees perceiving ITS as surveillance tool allowing management to see what, when, and how they work may became reluctant to use it or seek ways around the features generating these frustrations. For example, a work time tracking system implemented in an administrative environment could accurately pinpoint each employee's log ins and log outs and check if the computer is used in between, what applications are opened, what files are changed, and so on. Before rushing to implement such an "objective" supervisor, first assess its psychological effects on the employees.

Procedural rigidity and lack of commitment is generated in workplaces where the employees interact exclusively or mainly with their computer, using forms and procedures that require little, if at all, usage of their own rationing and creativity. It is the automated production line stress revisited, and almost all bad effects are similar: lack of commitment, alienation, frustration. Changing the looks and feel of work can address this problem, and the cause — ITS — can also provide the cure, or part of it. It suffice to add variety in procedures, forms, screens and activities to make work more enjoyable and eventually more productive.

Knowledge barrier or the new illiteracy puts highly educated people in the position to learn from formally uneducated computer geeks. It should not be a problem, but it becomes one when the skills needed to perform core tasks for the organization are not computer related. Take for example an expert mechanical designer, who used only the drawing board and put him in front of a computer running AutoCAD. He may never be able to adapt, and his expertise is lost to the organization. This barrier creates

problems when implementing dramatic changes of IT in the organization. If the users' knowledge was limited to procedures to follow in order to get their job done, new technology bringing new procedures leaves them with no qualification. Recruiting, hiring, training, promoting, career management, and retirement can all be affected by this knowledge barrier. Therefore an organization that includes computer training among the job amenities is more appreciated by current and prospective employees.

XII. DATA MANAGEMENT

The concept of data management is not about setting up databases, back-up procedures or storage devices. These aspects are specific to the technology used and may completely change when a new ITS is implemented. Instead, it focuses on issues involved in data acquisition, validation procedures and consistency of processing, which are not technology-specific aspects. The results provided by any IT system are as good as the data it processes. No matter how cutting edge is the technology used, how elaborated are the procedures or how well trained are the users, if data quality is poor, results will follow. Therefore it is a legitimate concern for managers to make sure the whole chain of data processing is fed with valid and reliable information.

Protection of data once it entered the system is an IT security issue, already discussed in chapter VIII. However, security methods and procedures do not distinguish between invalid and valuable data. Instead they attempt to protect everything. This means another mechanism must be in place to cope with data acquisition and ensure only correct, current and relevant data gets to be accepted by the system.

A. DATA SOURCES

1. Classification Criteria

The first step to be taken in data management is to identify all the data sources and list the types, volumes and formats used by each source. A number of classification criteria can be used to systematize this information, identify specific problems and select the ways to tackle them. The following list exemplifies such criteria, but should be seen just as a template to be tailored to reflect the actual ITS considered. Data sources can be classified:

By their **position to the organization**:

- external
- internal.

By the **type of information** contained:

- Text: memos, articles, technical documentation, manuals
- Static images: diagrams, charts, pictures, drawings
- Animated graphics, with or without sound
- Recorded sound: speeches, presentations, adds
- Recorded video, with or without sound
- Live sound: radio stations broadcasts, audio teleconferences
- Live video: TV broadcasts, video teleconferences
- Multimedia: combination of two or more different media
- Web pages
- Other digital files: programs, data files, functional datagrams, error messages

By the **sensitivity** of information contained:

- Public
- Confidential
- Secret

By the **rhythm** of refreshing:

- Quasi-continuous
- Periodical

- When requested
- Random

By the **initiative of data acquisition**:

- Manual: user-controlled transfer
- Semi-automatic: needs user request to initiate transfer
- Automatic: data flows into the system without user intervention

By the **throughput** required (actual numeric values may vary):

- User-size channels (10 MB/s or less)
- Server-size channels (10-100 MB/s)
- Large throughput (more than 100 MB/s)

Other classification criteria can be defined and used in order to better capture and describe relevant particularities for the organization. Once the complete list of sources and their relevant characteristics is created, the next step is to examine the quality and quantity of data required and set in place methods to ensure the system will be fed with the correct data at the right inputs and the right time.

2. External Sources

The main characteristic of the external data sources is that they cannot be controlled by the organization. Therefore data management should be focussed on 1) selecting the best-suited sources, 2) creating appropriate input capabilities, and 3) validating entries.

Selection of external data sources is not a one-time event, but a recurrent process, because more recent or better-presented data may become available anytime, and taking

advantage of the advantages offered by new sources may yield competitive advantages. Let us consider for example a company using a market-oriented pricing mechanism for the services it provides. Gathering the most recent quotations and evaluations for similar services may be critical for each biding package they offer to potential customers, so identifying new and better sources of data on the Internet can make the difference between success and rejection.

A particularly thorny problem connected with external data source selection is finding relevant data on the Internet. Due to the way it evolved, the Internet is the exact opposite of a database, i.e. data is not ordered, nor structured, thus making searches to yield relevant results more as a matter of luck and intuition than rigor and clear criteria. Therefore, beware of data extracted by means of a single random search, because it may be outdated, irrelevant, or plainly wrong. A good external data source selection needs to be based on sufficient knowledge about the limitations of the respective data markets, and the Internet is no exception.

Channels used to acquire data from the external environment must provide effective and reliable connections to the respective sources. They also must be able to accept and transfer the needed data in the form supplied, with the necessary speed, accuracy, and reliability. For example, stock market quotations provided by a brokerage agency in a given format should be accepted by the data channel and transferred to the organization before their relevance expires, without errors, and with a guaranteed availability of 24 hours a day, seven days a week.

Validation procedures are the virtual gatekeeper who decides what, how much, when and how is external data allowed to enter the IT system. To be precise, validation

works above and beyond security measures, which only focus on the threats they are designed to avoid. The logical order is as follows: data presented at the designated entry in the system is firstly checked by the security system against all envisaged threats, then it is handed to the validation procedures to have the contents evaluated for relevance, accuracy, format, or other specific criteria. Unlike internal sources of data, which are designed and controlled by the organization, external sources may unexpectedly change formats, refreshing rhythms or other parameters which, while still acceptable for the security system, can disrupt internal processes if validation procedures do not prevent entry, make the necessary adjustments, or prompt human intervention to correct discrepancies.

3. Internal Sources

What differentiates internal sources from the external ones is that they are controlled by the organization. This means they can be created, designed, modified, and used according to the needed flows of information. Once it passed the specific validation process, data from external sources can be assimilated to internal data and treated as such. Inputs for the IT system may differ from the original data as far as location, time of availability, formats, or other parameters. Therefore several steps need to be taken to ensure relevant data is presented at the prescribed time and input port for processing: 1) source selection, 2) raw data gathering, 3) data formatting 4) validation 5) transport 6) storage and retrieval.

Internal data source **selection** means identifying the best spot to collect a given kind of data. Usually there are several choices within the organization, but the optimal collection point is unique. Optimization criteria are specific to the organization and to the

input examined. For example if the work time tracking application needs to now how long did each employee work during the day, the collection spot can be set at the gate, at each workplace, or on a given workstation for manual entry by an operator. A large organization would prefer the first or second solutions, maybe enhanced with peripheral devices to automatically read ID cards, while a small organization would opt for the third, for financial reasons.

Gathering raw data to feed to ITS may be straight forward with automated peripherals like laser scanners or card readers, but it can also be a hassle if documents have to be retyped, compiled from various sources, modified to fit a different format, and so on. Sometimes data comes from places where it is gathered with pen and clipboard, and has to go through manual entry operations. For such cases portable devices, like wireless inventory scanners, could avoid human errors, which accumulate from both gathering and entry operations.

Even with internal sources, the willingness to contribute with relevant data can be a significant issue at this point. If data is supposed to enter the system from users which do not have an incentive to provide it and they cannot be obligated to comply, then all technological capabilities may go to waste, for lack of input to process. For example, a state-of-the-art IT-supported knowledge base implemented in the late 80s by KPMG Peat Marvick didn't leave up to the initial expectations only because users proved to be reluctant to store sensitive information for the others to access anytime [Ref. 17]

Although input formats can be designed to closely emulate the natural structure provided by the data source, formatting may be necessary 1) to cope with data presented in formats other than electronic, 2) to ensure consistency of formats throughout the

system and 3) to effectively and efficiently use storage and communication capabilities. The purpose of data formatting it to put information in the desired form without affecting the contents. No data should be discarded at this time, but a preliminary classification of data can be implemented through the formats used. For example readings from an ID card reader checking access in a building may come as a succession of twelve digits. Formatting process could be set up to add a timestamp and a code describing the reader's location, thus creating a standard package of data which is similar to the ones entering the system from all the other readers.

Validation of input data from internal sources is less concerned with data formats, which are under the control of the organization, and focuses instead on human errors and wrong readings from the peripheral devices. Relevance of data is also a lesser concern, because the flows of information are designed to capture and process only information that is needed. Because connections to internal data sources can be bi-directional, the validation process can benefit of this feature and become interactive. Based on either the data received or supplementary information requested in interactive mode, validation process ends by 1) discarding all data 2) admitting relevant parts and discarding excess and 3) admitting data without changes or limitations. A particular problem connecting validation with access rights is to decide in multi-access conflicts. For example, modification rights in a payroll database may be granted to several users. If two of them simultaneously try to make changes to the same record, the validation procedure should decide who's change takes precedence and warn the other his modifications are rejected. At a more elaborate level, validation may be set up to identify

and cope with contradictory information, either using a choice algorithm or prompting human intervention.

After examining data and choosing what goes and what not, the process must make a last decision and direct admitted data to the right recipient, using an internal addressing system.

Data transport within the ITS is straight forward if the whole organization is located in a single site (building or campus) supported by a LAN or interconnected LANs, and all workstations share the same operating system (OS), communication software and network protocols. A system composed of LANs based on various protocols and OS makes things more difficult, but it all comes to a translation issue. However, organizations using unconnected subsystems, global roaming users, WANs, VPNs, or wireless networks, need to look into data transport problems more closely, because delays, alteration or data loss are more likely to occur, and costs of data communications become significant and require optimization.

A general problem with all types of ITS is to determine the necessary throughput for each segment of the network, and to choose the technology to support it. This topic is closer examined in chapter VII but, as a general rule do not plan to build future features with today's specifications such as throughput or speed, because new applications push for more and more resources, communications included (Borland [Ref. 3]).

Data storage and retrieval should be considered from data management perspective as one of the key functions of ITS. Since several DBMS essentially tackle the same problem in different ways, each one claiming to be the best, technology selection could go into technical details that are not relevant to management. Some aspects are

sufficiently general to be valid across the board and their relevance towards the overall result calls for managerial consideration:

- Flexibility: how easy can future changes and needs be implemented without disruption.
- Dependence: how much external support is needed to customize and maintain the database.
- Interchangeability: how adaptive is the database to accept and deliver other than native formats.
- Custom packages: is DBMS a bundled package, or it can be custom-tailored.
- System restrictions: hardware or software limitations for future developments.
- TOC: estimated lifetime cost of using the respective DBMS.

B. VALIDATION PROCEDURES

Validation procedures must be designed to handle actual data they process, so they may largely vary in focus, technology, methods and adopted solutions. The following are some of the most common techniques used, listed here to illustrate the role of validation and possible approaches to it.

- Confirmation: refers to checking the received data in a dialog between the receiver and the sender, ranging from simple acknowledgement to full retransmission.
- Fingerprints: refers to identification data including with the payload in order to certify the origin of the received data. It is mainly used for security purposes, but may also apply to validation.

- Certification: is a technique using a third part that guarantees for the sender, so that the receiver can trust the information. Certification data can accompany the payload or it can be checked at the certifying party, as part of the validation process.

- Error checking: refers to additional data transferred in order to allow the receiver to check data integrity. The procedure is similar to sending a packing list, but may involve sophisticated algorithms to create and read the additional information.

- Cross-references: refers to checking the data against other source(s), including internal or previous readings.

- Templates: refers to fitting data into a predetermined structure, used as a reference.

- Time framing: refers to checking received data against predetermined time patterns.

- Manual examination: submitting data to a human operator authorization before accepting it.

XIII. MARKETING AND IT

Marketing in a non-IT organization focuses on the specific market for the products / services the organization offers. It may also look into upstream or downstream markets for data correlation and for diversification opportunities. If the IT industry is not one of these three markets, then it is considered out of scope for marketing. But what if the goods or services the organization produces include added value due to ITS, or competitive advantage is based on IT-supported capabilities? In this case the whole promotional mix should stress the competitive advantage, and marketing needs to promote IT as part of the product or service. A similar correlation can work in the other direction, from an IT-based market to the organization that needs to adapt in order to maintain its position or gain new advantages. These two directions of interaction define the external dimension of the relation between marketing and IT.

A. EXTERNAL MARKETING AND IT

Two major directions are the traditional focus for marketing: 1) information flows from and about the market and 2) flows of information from and about the organization, addressed to the market. The former is meant to build a realistic picture of customer needs, both current and forecasted, of competition and driving forces present on the specific market, to be used by management in decision-making processes. The latter is active, aimed to shape the way external environment perceives the organization and its products or services. There is also a transformational dimension attached to the second direction, in an attempt to anticipate, educate and influence attitudes and needs. IT can be seen as a mere tool for both interactions, but a closer look at the way things work would

reveal the fact that marketing actions are in turn shaped by ITS used, as far as their scope, objectives, means and functions.

The **scope** of traditional marketing actions is restricted to actual and prospective customers, and sometimes the relevant communities. Costs associated with market surveys and promotional mix prevent traditional marketing from expanding and try cover remote markets, with low probability of immediate results. Because of its global reach, IT allows comprehensive market surveys to encompass global sources with low costs and high degree of accuracy. Unconventional, IT-based components — such as e-sweepstakes, online banners and so on — included in the promotional mix can virtually reach any market segment and require smaller budgets than traditional media.

The **objectives** targeted by marketing actions may vary according to the organizational strategy: defense, consolidation, conquest of new market segments and so on. IT may add new objectives or reshape the existing ones. Let us consider for example the changes induced by e-commerce to the marketing objectives. Global presence, for example, becomes attainable through a simple virtual storefront that may expand business geographically and expand the typology of potential customers.

The **means** used in marketing are enriched with new IT-based tools and capabilities:

- Data mining and searches conducted on the Internet about the specific market.
- Internet-based pools and surveys.
- Organizational web site for image and product promotions.
- Direct marketing by e-mail.

- Virtual newsletters and electronic publications.
- Digital graphic design for materials to be used with other media.
- Electronic presentations including graphics, video, animations and sound.
- Promotional materials on CDs or floppy disks to be handed or sent.
- Banners and other forms of advertising on the Internet, especially on the portal sites.
- Virtual sweepstakes, raffles, and other promotional actions.
- Customer feedback on the products/services in electronic form.

Most marketing **functions** and events can be implemented on the Internet and enhanced as far as speed and richness of information. Here are some examples (Ellsworth [Ref. 5]):

- Product announcements.
- Product flyers or introductory information.
- Product specifications and data sheets.
- Pricing information.
- Catalogs.
- Events and demos.
- Free samples.
- Company contacts.
- Customer support.
- Promotional notices of special sales, etc.

- Documentation and manuals.
- Multimedia productions.
- Marketing or customer surveys and needs assessments.
- Product performance data.
- Service evaluations.
- Reviews and product commentary.
- Customer service information and functions.

B. INTERNAL MARKETING FOR IT

Transition towards a new ITS can be disruptive for the employers, especially when 1) the work was previously done in more traditional ways, 2) users feel they lose control over the information and knowledge they were praised for, 3) job security is threatened and 4) the new system requires re-training or more specialized skills. If that is the case, above and beyond the measures aimed to bring users' knowledge to the desired level, it is a good idea to set up and pursue an internal promotional campaign aimed to make employers buy into the new system.

Methods and techniques available to managers for such purpose can safely be borrowed from the arsenal of the marketing campaigns targeting potential customers. The only differences between this internal action and the traditional marketing mix are the subjects and the product offered. In this case, promotional actions focus on employees and the product is the new ITS.

Time is a critical factor for success. Once the main features of the new ITS are outlined and potential factors susceptible to make users reluctant are identified, the

promotional process should be started, before implementation actually begins. Here are a few aspects to consider in setting up the internal campaign:

- Point out the shortcomings of the current system that the new one addresses.
- Present the overall improvements targeted by the change.
- Depict workplace improvements, no matter how small.
- Set and present incentives for employees to actively support implementation.
- Describe the training process established to cope with the new knowledge required.
- Involve future users in details of implementation by gathering feedback.
- Identify and depict personal growth with the new system.

Reluctance of the employees to buy into the new ITS can be spawned by lack of first-hand information. Assumptions about the way their work is going to be affected can create feelings of insecurity and rejection. It is a good idea to organize informative presentations in order outline advantages and address concerns before they impinge on attitudes. Other means like circulars, memos, billboards, group e-mails, fliers and newsletters can be used for the same purpose.

C. ORGANIZATIONAL WEB SITE

Most, if not all, marketing functions listed above as suitable to be implemented on the Internet use the organizational web page (OWS) as their basis or entry portal. Some organizations may even use OWS as the main interface with the external environment. Amazon.com or Yahoo for example interact with hundred of thousands of users without a brick-and-mortar storefront. While virtually all organizations eventually get to a point

where OWS becomes a necessity, seen from the perspective of the role OWS plays in their business they all fit into one of the following three categories: 1) OWS is used a marketing instrument, but it supports no business transactions, 2) OWS carries part of the business, while traditional structures cover the rest and 3) OWS support all the business, while the physical organization supports OWS.

The first group includes organizations that use OWS as an extension of the traditional means used for institutional image promotion, news releases, public relations, job posting and so on, but actual sales are conducted or services provided exclusively in a physical environment. Looking at this category one may infer the role of OWS is secondary and consider it no more significant than any other media. However, the line between an IT-based business and a traditional one is not that clear. Let us consider for example the effects of goodwill on the bottom line. Since public perception of the organization — which sets the value of goodwill — is proven to affect prices and sales volume, then any factor that is susceptible to boost public image can produce financial effects. Given its large audience, flexibility of conveyed message and accessibility, OWS can be a strong influential factor in shaping public image, thus yielding tangible effects. In fact, organizations in this category are more or less in a continuous transition towards the next group, because a simple decision like migrating customer service to the OWS puts part of the business on this IT resource and subtracts responsibilities from the physical structures which used to carry on that function.

The second group is more stable, because many organizations simply need to interact with the environment on the physical level in order to provide the products and services they produce, and OWS is used to cover only functions dealing exclusively with

information. As a result of expanding technological capabilities and the dynamics of virtual market, functions that used to me handled by brick-and-mortar structures do migrate to OWS, but there is a limit to this tendency, imposed by the specifics of each business. A particular type of mix between virtual and physical structures uses both to simultaneously cover the same functions. There is no prescribed proportion for such situations, so managerial consideration should identify the best approach for each case.

The third group includes a relatively new breed of organizations built around a business that is completely web-based. Roles are reversed in this case, as IT is no longer a simple support but the core capacity, while the rest of the company provides support to the virtual presence. Not all types of business can work in this model, because products or services that require direct interaction with the customer — like construction, manufacturing, or transport — are obviously stuck in the previous group. However, recent developments in communications and Internet infrastructure encouraged migration of traditional businesses from traditional to virtual environments, in areas previously reserved to physical interaction. Education, consulting, staffing/recruiting, bookkeeping, and publishing services are examples of industries where virtual organizations penetrated the respective markets and successfully compete against traditional ones.

The process of setting up an OWS is driven by its purpose. If the organization plans to implement on the web a segment of the marketing mix and no business segments, then the marketing department will act as the customer of OWS and set the requirements. Internal ITS can either provide all the competence needed or outsource this service, as a whole or parts of it. Diverse criteria can be used in order to divide into

homogeneous tasks the effort required for OWS implementation, but the usual way of apportion the work is: 1) design, 2) hosting and 3) updating.

OWS design is often seen as an one-time event and outsourced, in order to take advantage of graphic capabilities and expertise of specialized contractors, without the need to build in-house capabilities in this area. A word of caution, though: this phase may need to be revisited more often than expected, in order to keep up with emerging web technologies or reflect significant organizational changes.

Hosting OWS has become a business in itself, and many Internet service providers (ISP) bundle offers for this service with security capabilities that take the burden of protection from their customers. Unless the organization has strong IT capabilities and/or full control over the information behind OWS is key, it is a good idea to explore outsourcing this function to an ISP and focus on the contents, rather than the way the OWS is kept up. Although design and hosting OWS can be outsourced to the same contractor, it may not necessarily be the most convenient solution, and there is no technical impediment to split the two functions and use different contractors.

Updating a static OWS requires manual editing, which is both time consuming and inefficient. Moreover, interaction with the user is limited to data stored within the source code of the respective web page. Therefore, it is a good idea to build the OWS as the user interface to a database, which makes it dynamically connected to the information stored behind the visible layers. In this case, the organization can update the information in the database without revisiting the design phase and independently from the hosting service.

Although the functions and phases involved in building, publishing, administering and maintaining the OWS in case e-business covers a significant part of the organization's strategic mission, the complexity of the issues involved require in this case to either create strong in-house IT capabilities, or seek comprehensive outsourcing agreements, preferable in partnerships.

D. E-BUSINESS

E-business has become omnipresent and nearly as essential to commerce as the telephone. For all intents and purposes, you can't compete nowadays without some kind of e-business strategy. The concept behind e-business is essentially to create a virtual storefront able to perform the functions of a regular brick-and-mortar store — e.g.. to display products/services, provide information on the features and benefits, support electronic transactions, get feedback from customers and provide customer support — taking advantage of the features offered by IT. The problem is, it never works this simple. Looking at e-commerce as it was just another store results in wasting money and effort with no payoff. According to a study published by the Gartner Group, 75 percent of e-business projects will likely fail to meet their objectives through 2002, because of fundamental flaws in project planning and management (Gartner Group [Ref. 11]). This is the effect of moving into a new business environment with traditional managerial principles. Successful e-business strategy—whether it's business-to-business or business-to-customer — must rely on systems that are fast, agile, scalable, reliable and well-managed. Managers of the e-business component of an enterprise must cope with rapid change, corporate experimentation, new and ever-shifting Internet technologies, and the

expectations of visitors from virtually anywhere. Here are some of the specific managerial issues raised by e-business:

- Extended public exposure: e-business applications are public-facing, so any mistakes are immediately displayed, possibly to a huge audience. Unauthorized or incorrect content and links can have financial and/or legal implications.

- High availability expectations: e-business demands 24 hours a day, seven days a week availability, as customers are a click away from the competitor's site, and global access means dropping schedules based on time zone considerations.

- Dynamic scalability: customer demand is difficult to estimate or control on the web, because virtually anyone can be a customer. E-business applications may be called upon to handle sudden surges of activity, making scalability especially crucial. Having the virtual storefront stalled because of customer traffic overflow is the acme of irony.

- Different security issues: putting valuable inventory and financial transaction capabilities on the web means inviting hackers, and you just cannot afford to treat IT security lightly and still remain in e-business.

- Increased complexity: e-business, by its nature, increases application complexity. It may require deploying a hyperlinked application with tens of thousands of files, linked to external sites, and to a changing array of web servers, all connect with internal systems, which can involve various databases, applications and legacy technologies.

- Comparable performance: you just cannot succeed with an e-business site working significantly slower or having poorer features than the competition. Since the market is global, so are the required standards of performance. Customers will not wait for a slow picture download, nor waste time on protracted electronic transactions. They just go elsewhere, since the cost to substitute is just a mouse click.

- Harder to control: maintaining managerial involvement in e-business processes requires more than just forging strategies and looking at the results. It requires a genuine understanding of the inner mechanisms and factors governing the flows of resources in the system and the ways it interacts with the environment.

The novelty and dynamic changes of this field did not allow a unique recipe for success to emerge. Instead, here are some mistakes to avoid[1]:

- Failing to think e-business projects all the way through. E-business should not be considered as an extension of the existing brick-and-mortar establishment. Instead, it needs to be treated as a new direction for diversification and set up as such, in every detail.

- Underestimating the degree of cultural change that is required. IT can induce major organizational changes, but moving into e-business means a new philosophy of interaction with the environment

- Thinking of competitors in the old way. According to a Gartner Group report [Ref. 11], "A company that develops an e-business plan using a list of existing

[1] Adapted after [16]

competitors runs a substantial risk of being blindsided." This is a new way of doing business, and it requires new ways to look at it.

- Mismanaging the mix. The traditional business model and e-business model must coexist, but the exact proportion between the two is specific for the organization and its environment.

- Failing to protect the brand. Many companies have different web sites, with different tools for each of the company's divisions. This means creating multiple messages, which may confuse the audience. Specifics of regional or functional divisions must be framed in the organizational background.

- Thinking technology is a panacea. Just having an e-business system supported by the most expensive or up-to-date technology available doesn't necessarily mean it covers all possible needs. There are limitations associated with IT, so expectations must be reasonable and based on actual specifications of the system.

- Don't be so afraid of making a mistake that you do nothing. Avoiding to engage the organization in e-business just because IT security issues or e-business complexity makes them harder to control is a decision in itself: to stay aside from a business forecasted to reach by 2004 as much as 7 percent of forecast total global economy (Gartner Group [Ref. 10]).

XIV. CONCLUSIONS AND RECOMMENDATIONS

A. CONCLUSIONS

This study looks from a practical perspective at the issues facing managerial decision-making in non-IT organizations. It is an attempt to sort out the kind of information needed for the managers to 1) understand IT specific problems they have to deal with 2) get a sense of the constrains involved, 3) identify available approaches and 4) formulate their own questions they should ask in order to maintain control over ITS processes and results.

Significant conclusions can be summarized as follows:

- Despite its complexity and dynamic evolution, IT is manageable and should not be seen as an esoteric field reserved exclusively for specialists. ITS implementation and change are processes that can be structured and organized to keep results synchronized with organizational strategy.

- Methodologies and techniques used to cope with aspects such as investment decisions, quality assurance, outsourcing or cost analysis in other organizational areas can also be applied to IT, if proper consideration is given to specific features of this field.

- Security issues of ITS should be a major managerial concern at conceptual level and become a matter of technology only insofar as the actual solutions adopted for implementation, administration and maintenance processes.

- Human resource aspects related to IT people in a non-IT organization raise specific problems that need to be identified and addressed before they affect performance.

- IT performance evaluation and benefit analysis are not beyond measurability, an appropriate set of metrics, methodologies and procedures can be set up to cope with these aspects and produce relevant information for each level of managerial decision-making in the organization.

- Because IT should closely emulate and support organizational information flows, any model used for analysis and prediction needs to be customized to reflect what is specific for the organization, keeping in mind that a general model can only yield general results.

- IT has a transformational effect on the organization as a whole and people as individuals and the kind of changes it induces can be predicted, influenced, alleviated, but not avoided completely.

- Data needed for all processes supported by IT should be managed as any raw material that enters and goes through various processes in the organization, i.e. subjected to an optimizing effort along the path from its acquisition or creation to the final distribution of results to users.

B. RECOMMENDATIONS FOR DOD

Although within DoD there are specialized structures that produce IT services, such as R&D, procurement, implementation, upgrading, maintenance and retirement of IT, most defense organizations are consumers of such services and fit into the category of non-IT organizations. Therefore they need to cope with the areas of managerial concern discussed in this study. Because of its degree of generality, the study is not directly applicable to any specific organization. Instead it offers an outlook of the processes

involved and can be used as the starting point and guideline for particular studies or actual projects in this field.

Another possible use of this material is for training purposes of operational and middle management levels, either in formal education establishments, or by periodic courses, presentations, workshops and so on. Particular non-IT organizations, where problems discussed here are, or should be, part of the managerial dashboard used to gauge and control the IT-related processes in the organization could benefit from adapting the methods and conclusions presented here to their specifics and turn this theoretical study into a working toolkit.

C. SUGGESTED FURTHER STUDIES

The scope of this study was intentionally limited to cover only those areas where the author could bring personal contribution based on experience. However, some areas not covered here may be of interest and could shed light on related issues, in order to offer a complete picture on the IT-related managerial concerns that need to be addressed. Here are a few examples:

- Accounting for IT assets, including equipment, software, licenses and copyrights.
- Specific effects of using IT-based products and services for accounting and materiel management purposes.
- Trends and organizational effects of the integration between communications and IT.

- Benefits and risks of Executive Information Systems (EIS) for the decision-making processes.

- Effects of specific limitations imposed by contracting regulations — such as FAR or DFARS — on the quality of IT systems implemented or changed.

- Specific constrains imposed in case of ITS for organizations with permanent or periodic needs for redeployment in remote location on a global scale.

- Inter-organizational cooperation in large IT projects.

XV. ANNEXES

A. SUMMARY OF CONTRACT TYPES FEATURES

CONTRACT FEATURES

	FIRM FIXED PRICE (FFP)	INDEFINITE DELIVERY (ID)	FIXED PRICE ECON. PRICE ADJUSTEMENT (FPEPA)	FIXED PRICE AWARD FEE (FPAF)	FP PROSPECTIVE REDETERMINABLE (FPPRD)
PRINCIPAL RISK TO BE MITIGATED	None. Costs can be estimated with a high degree of confidence. Thus, the contractor assumes the risk.	At the time of award, delivery requirements are not certain. Use: - Definite Quantity (if the required quantity is known and funded at the time of award). - Indefinite Quantity (if the minimum quantity required is known and funded at award). - Requirements (if no commitment on quantity is possible at award).	Market prices for required labor and/or materials are likely to be highly unstable over the life of contract.	Acceptance criteria are inherently judgmental, with a corresponding risk that the end user will not be fully satisfied.	Costs of performance can be estimated with confidence only for the first year of performance.
USE WHEN	- The requirement is well defined - Contractors are experienced in meeting it. - Market conditions are stable. - Financial risks are otherwise insignificant.		The market prices are severable and significant. The risk stems from industry-wide contingencies beyond the contractor's control. The dollar at risk outweigh the administrative burdens of an FPEPA.	Judgmental standards can be fairly applied by an Award Fee panel. The potential fee is large enough to both: - Provide a meaningful incentive. - Justify the administrative burdens of an FPAF.	The Buyer needs a firm commitment from the contractor to deliver the supplies or services during subsequent years. The dollars at risk outweigh the administrative burdens of an FPPRD.
ELEMENTS	A firm fixed price for each line item or one or more groupings of line items.	- "Per unit" price. - Performance period. - Ordering activities and delivery points - Maximum or minimum limit (if any) on each order. - Extent of each party's commitment on quantity.	A fixed price, ceiling on upward adjustment, and a formula for adjusting the price up or down based on: - Established prices. - Actual costs of the labor or materials. - Labor or material indices.	- A firm fixed price. - Standards for evaluating performance. - Procedures for calculating a "fee" based on performance against the standards.	- Fixed prices for the first period. - Proposed subsequent periods (at least 12 months apart). - Timetable for pricing the next period(s).
THE CONTRACTOR MUST	Provide an acceptable deliverable at the time, place, and price specified in the contract.	Provide acceptable deliverables at the per unit price when and where specified in each order, within the contractual ordering limits.	Provide an acceptable deliverable at the time and place specified in the contract at the adjusted price.	Perform at the time, place, and the price fixed in the contract.	Provide acceptable deliverable at the time and place specified in the contract at the price established for each period.
CONTRACTOR INCENTIVE (other than maximizing Goodwill)	Generally makes a dollar of profit for every dollar that costs are reduced.	Generally makes a dollar of profit for every dollar that per unit costs are reduced.	Generally makes a dollar of profit for every dollar that costs are reduced.	Generally makes a dollar of profit for every dollar that costs are reduced; and earn a fee for satisfying the performance standards.	For the period of performance, makes a dollar of profit for every dollar that costs are reduced.
TYPICAL APPLICATION	Commercial supplies and services.	Long term contracts for commercial supplies and support services.	Long term contracts for commercial supplies during a period of high inflation.	Installation support service.	Long term production of spare parts for a major system.
PRINCIPAL LIMITATIONS (IN PARTS 16, 32,35,AND 52 OF THE FAR)	Generally not appropriate for R&D.	Per unit price may be FFP, FPEPA, FPPRD, or catalog/market based. If a Req. contract, must buy it from that contractor.	Must be justified.	Must be negotiated.	Must be negotiated. Contractor needs an adequate accounting system. Prompt redeterminations.
VARIANTS	Firm Fixed Price Level of Effort				Retroactive Redetermination.

FIXED PRICE INCENTIVE (FPI)	COST PLUS FIXED FEE (CPFF)	COST PLUS INCENTIVE FEE (CPIF)	COST PLUS AWARD FEE (CPAF)	COST OR COST SHARING (C/CS)	TIME & MATERIALS (T&M)
Labor or material requirements for the work are moderately uncertain. Hence, the Buyer assumes part of the risk.	Labour hours, labour mix, and/or material requirements (among other things) necessary to perform are highly uncertain and speculative. Hence, the Buyer assumes the risks inherent in the contract – benefiting if the actual cost is lower than the expected cost; losing if the work cannot be completed within the expected cost of performance. Some cost type contracts include procedures for raising or lowering the fee as an incentive for the contractor to perform at lower cost and/or attain performance goals.				
A ceiling price can be established that covers the most probable risk inherent in the nature of work. The proposed profit sharing formula would motivate the contractor to control costs and meet other objectives.	Relating fee to performance (e.g., to actual costs) would be unworkable or of marginal utility.	An objective relationship can be established between the fee and such measures of performance as actual costs, delivery dates, performance benchmarks, and the like.	Objective incentive targets are not feasible for critical aspects of performance. Judgmental standards can be fairly applied. The potential fee would provide a meaningful incentive.	- The contractor expects substantial compensating benefits for absorbing part of the costs and/or foregoing fee, or - The vendor is a nonprofit entry.	Costs are too low to justify an audit of the contractor's indirect expenses.
- A ceiling price. - Target cost. - Target profit. - Delivery, quality, and/or other performance targets (optional). - A profit sharing formula.	- Target cost. - A fixed fee.	- Target cost. - Performance targets (optional) - A minimum, maximum, and target fee. - A formula for adjusting fee based on actual costs and/or performance.	- Target cost. - Standards for evaluating performance. - A base and maximum fee. - Procedures for adjusting "fee", based on performance against standards.	- Target cost. - If CS, an agreement on the Buyer's share of the costs. - No fee.	- A ceiling price - A per hour labour rate that also covers overhead and profit. - Provisions for reimbursing direct material costs.
Provide an acceptable deliverable at the time and place specified in the contract at or below the ceiling price.	Make a good faith effort to meet the Buyer's needs within the estimated cost in the Schedule.				Make a good faith effort to meet the Buyer's needs within the "ceiling price".
Realizes a higher profit by completing the work below the ceiling price and/or by meeting objective performance targets.	Realizes a higher rate of return (i.e., fee divided by total costs) as total cost decrease.	Realizes a higher fee by completing the work at a lower cost and/or by meeting other objective performance targets.	Realizes a higher fee by meeting judgmental performance standards.	If CS, shares in the cost of providing a deliverable of mutual benefit.	
Production of a major system based on a prototype.	Research study	Research and development of the prototype for a major system.	Large scale research study.	Joint research with educational institutions.	Emergency repairs to heating plants and aircraft engines.
Must be justified & negotiated. Contractor needs an adequate accounting system. Targets must be supported by cost data.	Must be negotiated. Must be justified. The contractor must have an adequate accounting system. The buyer must closely monitor the contractor's work to ensure use of efficient methods and cost controls. There are statutory and regulatory limits on the fees that may be negotiated. Must include the applicable "Limitation of Cost" clause at FAR 52.232-20 through 23.				Must be justified and negotiated. The Buyer must closely monitor the contractor's work.
Firm or Successive Targets.	Completion or Term				Labor Hour

B. SUMMARY OF NETWORK TECHNOLOGIES

Networking means data communication. Also, modern voice and video signal communications are digitally mastered. Therefore, especially when looking at WAN level, the boundaries between network and communication technologies is so blurred that it is hard to say a particular feature belongs to one of the two fields.

Ethernet, one of the pivotal technologies that made LANs possible, was developed in the 1970s by Digital, Intel and Xerox. This original design is often referred to by the initials of its creators - DIX. Ethernet works by connecting all devices to the same cable. Usually, a host can just transmit whenever the cable is not is use. In the relatively uncommon case where two devices start transmitting at the same time, a *collision* occurs. Both senders then wait a random amount of time before transmitting again. In any case, every device on the cable can receive every packet, but discards all those not addressed to it. This scheme, one of many that can regulate access to a hardware medium, is referred to *CSMA/CD*, an acronym for Carrier Sense, Multiple Access / Collision Detect. The performance of any CSMA/CD network depends on several considerations, including the method of determining waiting time after a collision, the length of the cabling, the size of packets, and the amount of traffic. The Ethernet standard defines how silent times are determined, and the network engineers can seldom influence this feature anyhow. The remaining factors are summarized in the table below, though be aware that the standard places supplementary constraints (Comer [Ref. 4]).

Performance	Feature	What happens
Cable length	Short	Short cables reduce the chance of collisions, since electrical signals take less time to propagate between hosts
Packet size	Large	Large packets reduce the chances of a collision, since collisions can only occur during a fixed time window at the beginning of a packet
Amount of traffic	Light (< 20% capacity)	More traffic means more collisions; for standard 10 Mbit/s Ethernet, try not to exceed 2 Mbit/s on any single segment

The most common local area network alternative to Ethernet is a network technology developed by IBM, called **Token Ring** (Brain [Ref. 2]). Where Ethernet relies on the random gaps between transmissions to regulate access to the medium, Token ring implements a strict, orderly access method. A token ring network arranges nodes in a logical ring. The nodes forward frames in one direction around the ring, removing a frame when it has circled the ring once. The ring initializes by creating a token, which is a special type of frame that gives a station permission to transmit. The token circles the ring like any frame until it encounters a station that wishes to transmit data. This station then "captures" the token by replacing the token frame with a data-carrying frame, which encircles the network. Once that data frame returns to the transmitting station, that station removes the data frame, creates a new token, and forwards that token on to the next node in the ring. Token ring nodes do not look for a carrier signal or listen for collisions; the presence of the token frame provides assurance that the station can transmit a data frame without fear of another station interrupting. Because a station transmits only a single data frame before passing the token along, each station on the ring will get a turn to communicate in a deterministic and fair manner. Token ring networks typically transmit data at either 4 or 16 Mbps.

Fiber Distributed Data Interface (FDDI) is another token passing technology that operates over a pair of fiber optic rings, with each ring passing a token in opposite directions. FDDI networks offered transmission speeds of 100 Mbps, which initially made them quite popular for high-speed networking. With the advent of 100 Mbps Ethernet, which is cheaper and easier to administer, FDDI has waned in popularity (Brain [Ref. 2]).

Another significant network technology is **Asynchronous Transfer Mode** (ATM). ATM networks blur the line between local and wide area networking, being able to attach many different devices with high reliability and at high speeds, even across the country. ATM networks are suitable for carrying not only data, but voice and video traffic as well, making them versatile and expandable. While ATM has not gained acceptance as rapidly as originally predicted, it is nonetheless a solid network technology for the future (Brain [Ref. 2]).

Digital Subscriber Line (DSL) is a family of technologies technology for bringing high-bandwidth information to homes and small businesses over ordinary copper telephone lines. xDSL refers to different variations of DSL, such as ADSL, HDSL, and RADSL. Assuming your home or small business is close enough to a telephone company central office that offers DSL service, you may be able to receive data at rates up to 6.1 megabits (millions of bits) per second (of a theoretical 8.448 megabits per second), enabling continuous transmission of motion video, audio, and even 3-D effects. More typically, individual connections will provide from 1.544 Mbps to 512 Kbps downstream and about 128 Kbps upstream. A DSL line can carry both data and voice signals and the data part of the line is continuously connected. DSL installations

began in 1998 and will continue at a greatly increased pace through the next decade in a number of communities in the U.S. and elsewhere. Compaq, Intel, and Microsoft working with telephone companies have developed a standard and easier-to-install form of ADSL called G.Lite that is accelerating deployment. DSL is expected to replace ISDN in many areas and to compete with the cable modem in bringing multimedia and 3-D to homes and small businesses (Tech Target.com, Inc. [Ref. 29]).

Integrated Services Digital Network (ISDN) is a set of standards for digital transmission over ordinary telephone copper wire as well as over other media. Home and business users who install ISDN adapters (in place of their modems) can see highly-graphic Web pages arriving very quickly (up to 128 Kbps). ISDN requires adapters at both ends of the transmission so your access provider also needs an ISDN adapter. ISDN is generally available from phone companies in most urban areas in the United States and Europe. There are two levels of service: the Basic Rate Interface (BRI), intended for the home and small enterprise, and the Primary Rate Interface (PRI), for larger users. Both rates include a number of B (bearer) channels and a D (delta) channel. The B channels carry data, voice, and other services. The D channel carries control and signaling information. The Basic Rate Interface consists of two 64 Kbps B channels and one 16 Kbps D channel. Thus, a Basic Rate user can have up to 128 Kbps service. The Primary Rate consists of 23 B channels and one 64 Kpbs D channel in the United States or 30 B channels and 1 D channel in Europe. ISDN in concept is the integration of both analog or voice data together with digital data over the same network. Although ISDN is integrating these on a medium designed for analog transmission, broadband ISDN (BISDN) extends the integration of both services throughout the rest of the end-to-end

path using fiber optic and radio media. Broadband ISDN encompasses frame relay service for high-speed data that can be sent in large bursts, the Fiber Distributed-Data Interface (FDDI), and the Synchronous Optical Network (SONET). BISDN supports transmission from 2 Mbps up to much higher, but as yet unspecified, rates (Brain [Ref. 2]).

Frame relay is a telecommunication service designed for cost-efficient data transmission for intermittent traffic between local area networks (LANs) and between end-points in a wide area network (WAN). Frame relay puts data in a variable-size unit called a frame and leaves any necessary error correction (retransmission of data) up to the end-points, which speeds up overall data transmission. For most services, the network provides a permanent virtual circuit (PVC), which means that the customer sees a continuos, dedicated connection without having to pay for a full-time leased line, while the service provider figures out the route each frame travels to its destination and can charge based on usage. An enterprise can select a level of service quality - prioritizing some frames and making others less important. Frame relay is provided on fractional or full T-1 carriers. Frame relay complements and provides a mid-range service between ISDN, which offers bandwidth at 128 Kbps, and Asynchronous Transfer Mode (ATM), which operates in somewhat similar fashion to frame relay but at speeds from 155.520 Mbps or 622.080 Mbps.

Frame relay is based on an older packet-switching technology which was designed for transmitting analog data such as voice conversations. Unlike protocols designed for analog signals, frame relay is a fast-packet technology, which means that the protocol does not attempt to correct errors. When an error is detected in a frame, it is

simply "dropped." (trown away). The end points are responsible for detecting and retransmitting dropped frames. (However, the incidence of error in digital networks is extraordinarily small relative to analog networks.) Frame relay is often used to connect local area networks with major backbones as well as on public wide area networks and also in private network environments with leased lines over T-1 lines. It requires a dedicated connection during the transmission period. It's not ideally suited for voice or video transmission, which requires a steady flow of transmissions. However, under certain circumstances, it is used for voice and video transmission (Brain [Ref. 2]).

C. NETWORK PERFORMANCE PARAMETERS (Freeman [Ref.9])

Throughput is defined as the measurement of the number of bits that can be transmitted through a network over a specified period of time. Performance will be measured in million bits per second (Mbps). Throughput is also wrongly referred to as bandwidth.

Jitter is short-term, intra-packet (or intra-cell) instability of an electrical signal caused by electrical or mechanical changes.

Utilization is the measurement of traffic usage on a network and is expressed as a percentage. Ethernet utilization is determined by measuring the amount of network traffic on a segment for a specific period of time compared to the total potential of 10.

Latency s the amount of time it takes for a packet to go from one point to another. Latency is measured in milliseconds (ms).

Packet Loss is defined as the measurement of the number of packets that be are dropped in a network over a specified period of time. Packet Loss will be measured in dropped packets per second or percentage.

Bit Error Rate (BER) / **Cell Error Rate** (CER): The ratio between the total number of bits (cells) transmitted in a given message and the number of bits in that message received in error. A measure of the quality of a data transmission, usually expressed as a number referred to a power of 10; e.g., 10

LIST OF REFERENCES

1. Albert,S, *Web Hosting: The new Face of IT Outsourcing,* http://outsourcing.com/howandwhy/articles/webhosting/main.htm
2. Brain, Marshall, *How Stuff Works,* http://www.howstuffworks.com
3. Borland, J., *Living Up to the Broadband Hype,* CNET News.com, July 28, 1999, http://news.cnet.com/news/0-1004-201-343780.html
4. Comer, Douglas, *Computer Networks and Internets,* Prentice Hall, 1999.
5. Ellsworth, J., *The Internet Business Book,* John Willey & Sons, 1994.
6. Everest Group, *Redefining Outsourcing: The Value Model,* 1999, http://www.outsourcing-mgmt.com/banners/everest/redefiningoutsourcing.pdf
7. *Findings of Fact*, Civil Action No. 98-1232 (TPJ), U.S. versus Microsoft Corporation, http://usvms.gpo.gov/ms-findings2.html
8. Fred Cohen, *Managing Network Security: How Good Do You Have To Be? http://www.all.net/*
9. Freeman, Ken and Chow, Doris, *Network Monitoring,* http://www.nren.nasa.gov/eng/freeman/performance/tsld001.htm
10. Gartner Group, *Triggering the B2B Electronic Commerce Explosion,* April 3, 2000, http://gartner12.gartnerweb.com/ggbin/ggtoc
11. Gartner Group, *CEO and CIO Alert: Five Mistakes That Will Derail an E-Business Project,* Aug. 1999, http://gartner12.gartnerweb.com/public/static/home/home.html
12. General Services Administration, *Federal Acquisition Regulation,* http://www.arnet.gov/far
13. Grice, C, *The pitfalls of High Speed Installs,* CNET News.com, 1999, http://news.cnet.com/news/0-1004-201-343782-0.html
14. Haga, William, *Management of Information Systems – Course Notes*, Naval Postgraduate School,1999.
15. Hirschheim, R, *Backsourcing, An Emerging Trend?, in Outsourcing Journal, http:www.outsourcing-academics.com/html/acad1.html,* 05/04/2000.
16. Hubbard, Douglas, *Everything Is Measurable, in: CIO Enterprise Magazine, Nov. 1997,* http://www.cio.com/archive/enterprise/111597_checks_content.html, 02/20/2000.
17. Harvard Business School, *Case Study 9-429-002, KPMG Peat Marwick: The Shadow Partner,* 1995.
18. Intel Corporation, *Three Vectors of Performance,* http://www.edtn.com/scribe/reference/appnotes/md007613.htm
19. Internet.com Corp., *PC Webopedia,* http://www.pcwebopaedia.com
20. International Society of Parametric Analysts, *Parametric Estimating Handbook,* http://www.ispa-cost.org/PEIWeb/cover.htm
21. Kelly, Floyd, *Performance Measurement: Achieving high performance through alignment and strategic learning,* http://www.ceoreview.com/papers/perfmeas.htm

22. Kodak Digital Learning Center, http://www.kodak.com/US/en/digital/dlc/book2/chapter4/flashp1.shtml

23. *Logistics Outsourcing,* Infoserver, Outsourcing Journal, Apr. 1999, http://www.outsourcing-journal.com/issues/apr1999/html/academic.html

24. NASA, *DSN Software development Handbook,* http://www-isds.jpl.nasa.gov/cwo/cwo_23/handbook/dsnswdhb.htm

25. Network Associates, Inc, *Introduction to Cryptography,* Network Associates, *1998*

26. Sewell, Meg and Marczak Mary, *Using Cost Analysis in Evaluation,* http://ag.arizona.edu/fcr/fs/cyfar/Costben2.htm

27. Standard Performance Evaluation Corporation, *Metrics Glossary,* http://www.specbench.org

28. Strickland, Thompson, *Crafting and Implementing Strategy,* Irwin McGraw-Hill, 1998.

29. Tech Target.com, Inc., *What Is?,* http://www.whatis.com/dsl.htm

30. Trowbridge, B., *Overcoming the Inherent Gridlock in Outsourcing, Outsourcing Journal,* http://www.outsourcing-journal.com/issues/dec1999/html/supplier2.html

BIBLIOGRAPHY

1. Ancona, Deborah, *Managing for the Future,* South-Western College Publishing, 1998.
2. Boardman, Anthony et al., *Cost-Benefit Analysis: Concepts and Practice,* Prentice Hall, 1996.
3. Baccala, Brent, *An Internet Encyclopedia,* http://cie.bilkent.edu.tr/index.htm
4. Borthick, Sandra, *Why We Can't Compare ISP Performance — Yet,* in Business Communications Review, Sept. 1998, http://www.bcr.com/bcrmag/09/98p35.htm
5. Buller, Paul and Schuler Randal, *Managing Organizations and People,* South-Western College Publishing, 2000.
6. Casselberry, Rich, *Running a Perfect Intranet,* Que Corporation, 1996, http://absolut.banki.hu/~asoka/www.mcp.com/818640000/0-7897/0-7897-0823-X/index.htm
7. David Cearley, *Get Real on Cost of Ownership,* in: CIO Magazine, Sept. 1997, http://www.cio.com/archive/090197_meta_content.html 02/20/2000.
8. Fred Cohen, *Managing Network Security: A Strategic View, http://www.all.net/*
9. Greenberg, Jerald, *Managing Behavior in Organizations,* Prentice Hall, 1999.
10. John Barkley, *Security in Open Systems, in:National Institute of Standards and Technology, Special Publication 800-7/1994, http://csrc.ncsl.nist.gov/nistpubs/800-7/node9.html*
11. Krippendorff, Klaus, *A Dictionary of Cybernetics, in: F. Heylighen, C. Joslyn and V. Turchin, Principia Cybernetica Web, Principia Cybernetica, Brussels, http://pespmc1.vub.ac.be/ASC/OPEN_SYSTE.html*
12. Mansfield, Edwin, *Applied Microeconomics,* W.W. Norton & Co., 1997.
13. Monua Janah, *The Cost of Networking, in: Information Week, Oct. 1998, http://www.informationweek.com/705/05iunet.htm,02/20/2000*
14. Oberlin, John, *Departamental Budgeting for Information Technology: A Lifecycle Approach,* http://www.educause.edu/ir/library/text/CEM9424.txt
15. Resource Management Systems Inc., http://www.rms.net/index.shtml
16. Rowe, Randi., *Keeping the business in e-business,* http://www.techrepublic.com/article.jhtml?id=/article/r00519991207row01.htm
17. *Sample Information Technology Performance Measures,* http://www.itpolicy.gsa.gov/mkm/pathways/samp-it.htm
18. Stallings, William, *Operating Systems – Internals and Design Principles,* Prentice Hall, 1998.
19. U.S. DoD Information Technology Standards Guidance (ITSG) http://www.ada.pair.com/itsg/INTROV31.htm
20. Ubois, Jeffrey and Teach, Edward, *Pipe Dreams, in: CFO Magazine, Mar. 1999, http://www.cfonet.com/html/Articles/CFO/1999/99MApipe.html*

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center 2
   8725 John J. Kingman Road, Ste 0944
   Fort Belvoir, VA 22060-6218

2. Dudley Knox Library 2
   Naval Postgraduate School
   411 Dyer Road
   Monterey, California 93943-5101

3. Professor William J. Haga, Code SM/Hg 1
   Naval Postgraduate School
   Monterey, CA 93943

4. Professor Roger Evered, Code SM/Ev 1
   Naval Postgraduate School
   Monterey, CA 93943

5. MAJ Gabriel V. Ana 1
   Departamentul Inzestrarii Armatei
   Drumul Taberei 9-11, Sector 4
   Bucharest, ROMANIA

6. Gabriel V. Ana 1
   11, Vatra Dornei ST. BL18 B+C, SC.4, ET.3, AP.148
   Sector 4, 75529
   Bucharest, ROMANIA