A PROTOTYPE SYSTEM OF ICT SECURITY MEASUREMENT USING BALANCED SCORECARD

ORATHAI UNGAMRUNG

A RESEARCH PROJECT SUBMITTED IN PARTIAL
FULFILLMENT OF THE REQUIREMENTS FOR
THE DEGREE OF MASTER OF SCIENCE
(COMPUTER SCIENCE)
FACULTY OF GRADUATE STUDIES
MAHIDOL UNIVERSITY
2007

Research Project
Entitled

A PROTOTYPE SYSTEM OF ICT SECURITY MEASUREMENT USING BALANCED SCORECARD

…….
Miss Orathai Ungamrung
Candidate

…….
Assoc. Prof. Supachai Tangwongsan, Ph.D.
Major-Advisor

…….
Assoc. Prof. Damras Wongsawang, Ph.D.
Co-Advisor

…….
Lect. Songsri Tangsripairoj, Ph.D.
Co-Advisor

……
Prof. M.R. Jisnuson Svasti, Ph.D.
Dean
Faculty of Graduate Studies

……
Assoc. Prof. Supachai Tangwongsan, Ph.D.
Chair
Master of Science Programme in
Computer Science
Faculty of Science

Research Project
Entitled

A PROTOTYPE SYSTEM OF ICT SECURITY MEASUREMENT USING BALANCED SCORECARD

was submitted to the Faculty of Graduate Studies, Mahidol University

for the degree of Master of Science (Computer Science)

on

May 31, 2007

…….
Miss Orathai Ungamrung
Candidate

……
Lect. Siwaruk Siwamogsatham, Ph.D.
Chair

……
Assoc. Prof. Supachai Tangwongsan, Ph.D.
Member

……
Assoc. Prof. Damras Wongsawang, Ph.D.
Member

……
Lect. Songsri Tangsripairoj, Ph.D.
Member

……
Prof. M.R. Jisnuson Svasti, Ph.D.
Dean
Faculty of Graduate Studies
Mahidol University

……
Prof. Amaret Bhumiratana, Ph.D.
Dean
Faculty of Science
Mahidol University

ACKNOWLEDGEMENTS

Finally, after finishing this research project, it is time to attend the part that, most possibly, will be the most read of all: the acknowledgements. This is no exception, as what the number of people that contributed to it is concerned and it is time to thank them for all they did for helping me to reach this goal.

To start with, I would like to express the deepest appreciation to my Professor Dr. Supachai Tangwongsan who has the attitude and the substance of a genius: he continually and convincingly conveyed a spirit of adventure in regard to research and an excitement in regard to teaching. Without his guidance and persistent help this dissertation would not have been possible. I also praise his observations and constructive suggestions concerning my research project.

I extend my heartfelt acknowledgement to all staff members of the Computer Science Department, Mahidol University.

Where would I be without my family? My parents deserve special mention for their inseparable support and prayers. My Father, Mr. Prinya Ungamrung in the first place is the person who put the fundament my learning character, showing me the joy of intellectual pursuit ever since I was a child. My Mother, Ms. Varaporn Ungamrung is the one who sincerely raised me with her caring and gently love. My sister and My brother thanks for being supportive and caring siblings.

Finally, I would like to thank everybody who was important to the successful realization of research project. Numerous friends for always unwavering support and understanding during the many hours I dedicated to achieving this milestone in my life and career as well as expressing my apology that I could not mention personally one by one.

Orathai Ungamrung

A PROTOTYPE SYSTEM OF ICT SECURITY MEASUREMENT USING BALANCED SCORECARD

ORATHAI UNGAMRUNG 4637280 SCCS/M

M.Sc.(COMPUTER SCIENCE)

RESEARCH PROJECT ADVISORS: SUPACHAI TANGWONGSAN, Ph.D., DAMRAS WONGSAWANG, Ph.D., SONGSRI TANGSRIPAIROJ, Ph.D.

ABSTRACT

The objective of this research was to design a prototype of an information and communication technology (ICT) security system within an organization, applying the balanced scorecard to the evaluation. Indicators used for the evaluation were gathered from ISO/IEC 17799, which is the international standard for ICT. They are multi-measure indicators, with a number of factors having an impact on these standards. As a consequence, the analytic hierarchy process (AHP) is used to analyze the evaluation measures, so that the measures derived are reliable and realistic. In addition, the evaluation result will be displayed in the form of scorecard to enable the executives to view the current situation of the ICT security within their organization.

For a trial of the prototype system, a medium-size bank in Thailand was applied as the prototype organization. Typically, banks have branches in provinces and districts throughout the country. In this connection, the bank's branches and regional centers were evaluated for their ICT security, by defining the weight and score of indicators for each branch. The weight and score defined for an evaluation could be adjusted based on appropriateness so that the outcomes obtained were realistic. Subsequently, the system would make an evaluation of the ICT security of the bank's branches and regional centers, including summarizing an assessment of the ICT security of provinces, regions and the organization itself. In this regard, an evaluation consequence was displayed in 2 patterns of scorecards, namely, tree and table. The data was revealed from the viewpoint of the bank's branches, regional centers, provinces, regions and organization.

The findings of the research reveal that the designed and developed evaluation prototype for ICT security within an organization can achieve the defined objectives.

KEYWORDS: BALANCED SCORECARD/ ICT SECURITY MEASUREMENT

115 P.

ระบบต้นแบบในการประเมินระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศโดยใช้ BALANCED SCORECARD (A PROTOTYPE SYSTEM OF ICT SECURITY MEASUREMENT USING BALANCED SCORECARD)

อรทัย อุงอำรุง 4637280 SCCS/M

วท.ม. (วิทยาการคอมพิวเตอร์)

คณะกรรมการควบคุมโครงการวิจัย : ศุภชัย ตั้งวงศ์ศานต์, Ph.D., ดำรัส วงศ์สว่าง, Ph.D., ทรงศรี ตั้งศรีไพโรจน์, Ph.D.

บทคัดย่อ

โครงงานวิจัยนี้ เป็นการออกแบบต้นแบบของการประเมิน ICT Security ภายในองค์กร ซึ่งได้ประยุกต์นำ Balanced Scorecard (BSC) มาใช้ในการประเมิน โดย Indicator ที่ใช้ในการประเมินได้ประมวลมาจาก ISO/IEC 17799 ซึ่งเป็น International Standard ที่เกี่ยวกับเทคโนโลยีสารสนเทศ สำหรับ Indicator นี้เป็นตัวชี้วัดแบบหลายเกณฑ์ และหลักเกณฑ์ต่างๆ มีหลายปัจจัยที่มีผลกระทบดังนั้นการวิเคราะห์จึงใช้วิธี Analytic Hierarchy Process (AHP) ในการวิเคราะห์เกณฑ์การประเมิน เพื่อให้เกณฑ์ที่ได้มีความน่าเชื่อถือ และสมจริงสมจัง นอกจากนี้ผลการประเมินจะแสดงในลักษณะของ Scorecard เพื่อให้ผู้บริหารเห็นสถานะปัจจุบันของ ICT Security ภายในองค์กร

ในการทดลองระบบต้นแบบ เราใช้องค์กรต้นแบบเป็นธนาคารขนาดกลางแห่งหนึ่งในประเทศไทย ซึ่งโดยทั่วไปธนาคารจะมีการขยายสาขาไปตามจังหวัด และอำเภอต่างๆ ทั่วประเทศ เราจึงทำการประเมิน ICT Security ของสาขา และศูนย์ภาคของธนาคาร โดยกำหนดค่า Weight และ Score ของ Indicator ในแต่ละสาขา อีกทั้งสามารถปรับเปลี่ยนค่า Weight และ Score ในการประเมินได้ตามความเหมาะสม เพื่อให้ผลที่ได้มีความสมจริงสมจัง จากนั้นระบบจะทำการประเมินผล ICT Security ของสาขา ศูนย์ภาค รวมถึงสรุปผลการประเมิน ICT Security ของจังหวัด ภาค และองค์กร และแสดงผลการประเมินในลักษณะ Scorecard 2 รูปแบบ คือ Tree และ Table โดยแสดงข้อมูลในมุมมองของสาขา ศูนย์ภาค จังหวัด ภาค และองค์กร

สรุประบบต้นแบบของการประเมิน ICT Security ภายในองค์กร ที่ได้ออกแบบและพัฒนาขึ้นสามารถบรรลุตามวัตถุประสงค์ที่ได้ตั้งไว้

115 หน้า

CONTENTS

CONTENTS (Cont.)

CONTENTS (Cont.)

LIST OF TABLES

Page

LIST OF FIGURES

Page

LIST OF FIGURES (Cont.)

Page

LIST OF FIGURES (Cont.)

Page

LIST OF FIGURES (Cont.)

Page

CHAPTER I
INTRODUCTION

Over the recent years, the principles and concepts of the balanced scorecard (BSC) and key performance indicators (KPIs) receive considerable attention from executives of both the public and private agencies. Initially, the awareness on the BSC began with the private sector, particularly by foreign companies doing business in Thailand. Subsequently, the BSC has gradually expanded to large Thai agencies. Currently, it starts to escalate to medium-size agencies and increasingly attracts more attention of sate agencies and enterprises.

The BSC is an instrument used for an evaluation, focusing on defining indicators and objectives intended to achieve, apart from transforming indicators at the organizational level into departmental and divisional levels or smaller work units, respectively. The BSC is not only a tool for an assessment but can also be used to transmute strategies into action plans. After the BSC is utilized until action plans are generated, performance consequences during different periods can be compared with the objectives defined, which enable an organization of what will happen. This make the BSC a supplementary tool for the managerial system within the organization, engendering an attribute of a self-sufficient cycle in it.

The principles of BSC are rather flexible and open and thus, depend on the characteristics of an organization and its executives to select an approach of developing the BSC appropriate for the organization itself.

This research project has applied the BSC to an evaluation of the ICT security within an organization. Indicators used for an evaluation are compiled from ISO/IEC 17799, which is the international standards for information technology (ICT). They

are multi-measure indicators. Consequently, the analytic hierarchy process (AHP) is used to analyze the evaluation measures, so that they are reliable and realistic.

The prototype agency used to evaluate the ICT security within its boundary is a medium-size Thai bank. Typically, domestic banks will expand their branches to provinces and districts across Thailand, causing them to have a wide variety of places and environments. To evaluate the ICT security of a bank, its branches throughout the country are assessed by defining the same indicators used to evaluate each branch. Nevertheless, since each branch differs in terms of location and environment, it thus defines the weight and score of indicators based on the actual condition of its location (ARCA). Similarly, each branch can adjust weight and score to suit an evaluation. This aims to get the most realistic evaluation consequence.

An experiment is conducted to assess the ICT security of the bank's branches and regional centers. Once the outcome of the branches and regional centers assessment is derives, the system will summarize it as a result of an ICT security evaluation for the provinces, regions and the organization as a whole. Of course, the result will be demonstrated in the form of a scorecard via the viewpoint of the branches, regional centers, provinces, regions and organization (bank) itself, to enable the bank's executives to view the current situation of the ICT security within the organization as a whole.

This research consists of 7 chapters, each with the following details.

Chapter 1: **Introduction** discusses an overview of the balanced scorecard, and its application to the research project.

Chapter 2: **Problem statement** discusses the motivation for developing a system of the ICT security evaluation for an organization, related works on the ICT security measurement, as well as the objectives and scope of the system development.

Chapter 3: **Conceptual design** reviews the nature of structure of the organization used as a model case study to measure the ICT security, a method of weight and score calculation, including an example of the design of a scorecard used to display an evaluation consequence.

Chapter 4: **Detailed design** elaborates on the detailed design of a system of the balanced scorecard for ICT security, consisting of use case diagram, class diagram, sequence diagram, file structure and module specification.

Chapter 5: **System implementation** discusses the system environment, system tools and resources, program structure and XML structure.

Chapter 6: **Experimental results** describes experimental consequences for the system of efficiency measurement of ICT security, consisting of measurement which defines the parameters used for an evaluation, and a scorecard which display the result of efficiency measurement of ICT security in the form of color.

Chapter 7: **Discussion and conclusion** discusses the development of this research project and concludes the system of efficiency measurement of the organization’s ICT security.

CHAPTER II
PROBLEM STATEMENT

This chapter discusses the motivation for developing a system of the ICT security evaluation for an organization, related works on the ICT security measurement, as well as the objectives and scope of the system development.

2.1 Motivation

- ICT security is an interesting topic. Security is an essential factor for organizations' success because security has major involvements to all aspects of organizations' processes. Thus, tightening security would help organizations to develop their management and administration.

- Applying balanced scorecard to ICT security is an innovative idea. The results of most security evaluation methodologies are based on numeric. The application of balanced scorecard would ease the evaluation processes due to its color-based evaluation results. Moreover, balanced scorecard provides users with indicators and objectives for comparing outcomes against objectives which facilitate management and executives.

- The problem of how-to is quite challenging. With the features of balanced scorecard's color-based evaluations, the implementation of evaluation results from numeric-based to color-based for the whole organization is rather a challenging subject.

2.2 Literature review

Related work in ICT security measurement as follow:

2.2.1 ISO/IEC 17799 [5]

ISO/IEC 17799 is international standard related to information and communication technology (ICT). This standard will advise about information security management which helps to increase efficiency in organization management security. The security standard which have to develop are:

- Security policy
- Organizational security
- Asset classification and control
- Personnel security
- Physical and environmental security
- Communications and operations management
- Access control
- Systems development and maintenance
- Business continuity management
- Compliance

2.2.2 Balanced scorecard

Robert Kaplan and David Norton [10] developed a management and measurement tool called the balanced scorecard (BSC). The BSC lists a diverse set of performance measures grouped in four categories:

- Financial Perspective
- Customer Perspective
- Internal Business Perspective

- Innovation and Learning Perspective

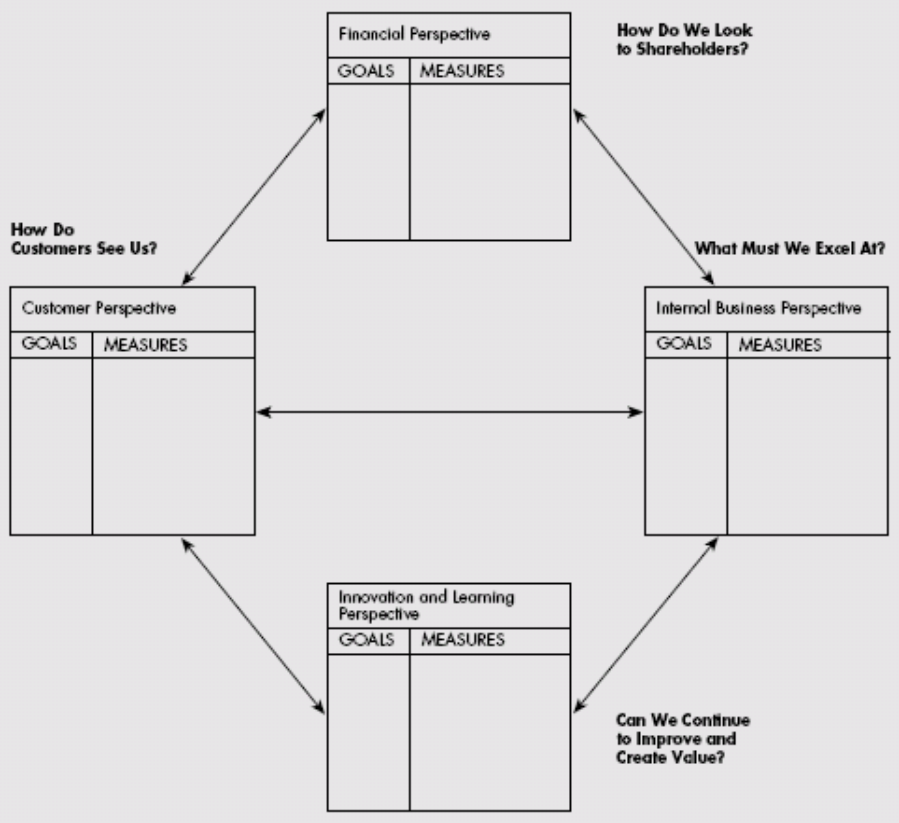

Figure 2.1 The balanced scorecard links performance measures

Figure 2.1 Shows relationship of perspective and identified goal and measure for each.

2.2.3 Implementation scorecard

Marlys Gascho Lipe and Steven Salterio [8] considering about efficiency of balanced scorecard in organization by use balanced scorecard to evaluate performance in many department. Experiment is comparing performance between 2 departments. The research used divide and conquer method which divided balanced scorecard to 4 perspectives (Financial, Customer-related, Internal business process, Learning and growth) and there are 20 measures in 4 perspectives. The experiment will compare between balanced scorecard and NOFORM. Evaluation used ANOVA (analysis of

variance) which is the result found that mostly good result always come from balanced scorecard.

Wim Van Grembergen and Ronald Saull [15] developed implement ICT balanced scorecard in information service department for 3 financial company in Canada by separate ICT scorecard framework to 4 parts are customer orientation**,** corporate contribution, operational excellence and future orientation by set objective, measures and benchmarks for 4 scorecard to evaluate performance of executive management, board of director and shareholder.

Objective	Measures	Benchmarks
Strategic contribution	• Completion of strategic initiatives	• Not applicable
Synergy achievement	• Completion of single system solutions • Achievements of Group synergies	• "Systems Map" • Bain & Co. targets
Business value of IT projects	• Business evaluation based on traditional financial measures (ROI, etc.) or Information Economics	• Company hurdle rate
Management of IT investments	• Actual versus budgeted expenses • Cost recovery versus expenses	• Expenditures relative to "selected" competitors

Figure 2.2 Example corporate contribution scorecard

Figure 2.2 Shows objective, measures and benchmarks of corporate contribution scorecard

Stan Davis and Tom Albright [12] studies for efficiency of balanced scorecard to improve financial performance for bank by comparing between the branch which has implement balanced scorecard and the branch with non implement balanced scorecard. Use CKFM (Composite Key Financial Measure) to measuring performance and set scale and weight in various environment of each branch. The result of experiment found that the performance of balanced scorecard branch is increasing.

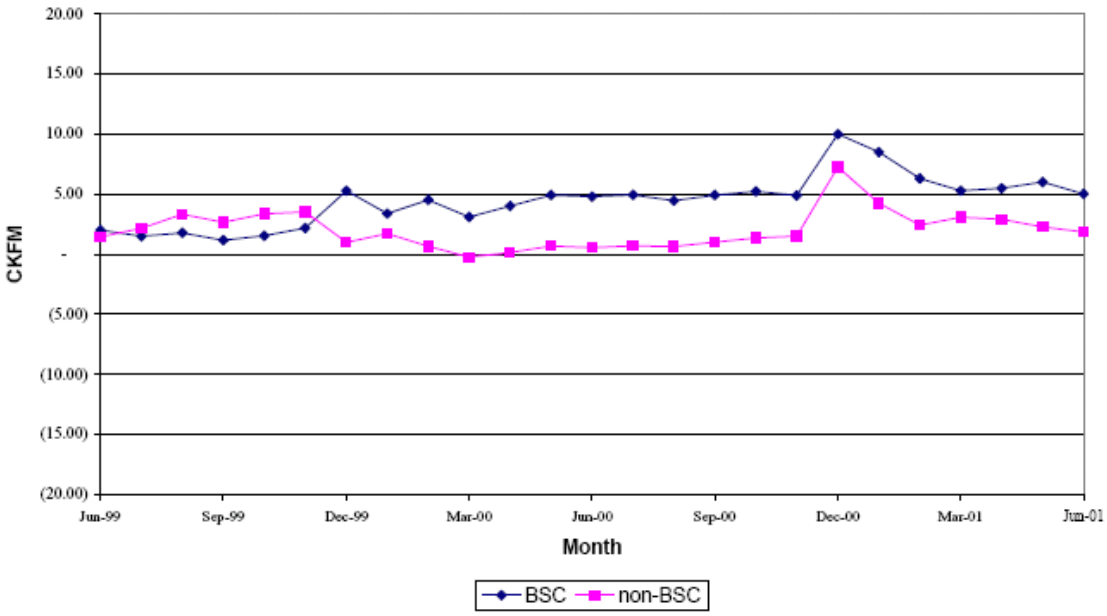

Figure 2.3 Graph of group median CKFMs over observation period for BSC and non-BSC branches.

Figure 2.3 indicates an increase in performance for BSC branches. The purpose of the statistical tests is to determine whether a significant increase in performance occurred from June 1999 to June 2001 for BSC and control division branches. In addition, the tests examine whether BSC branch performance increased significantly more than control division performance.

Volkmar H. Haase [14] use concept of balanced scorecard and decision support system (DSS) at based on fuzzy logic by create as software tool to help strategic business process optimize this system implement by input figures, indicators, mappings and function which is can improve and develop as needed as well as strategy.

Clemens Lohman , Leonard Fortuin and Marc Wouters [1] develop a prototype system for performance measurement and represented in scorecard form. The study took place at European Operations of Nike. The performance metric divided to 6 clusters. A scorecard structure with three layers (Top level, Mid level and

Lowest level) is used for displaying the information. In each layer will represent the difference level.

Erkan Kahraman [3] developed application for evaluation performance ICT security in organization with quantitative metrics to help in follow up progress of system. This research will evaluate under ICT security metrics which is separate to 4 groups are organization, operation, technical and people. The consequences of experiment will assist us make decision to ICT security investment.

1. Does the organization have a security policy developed?
To start with, there must be an existing Security Policy in order to be evaluated.
Method: Check List.
Evaluation: Yes (1), No (0).

Figure 2.4 Example check list

Figure 2.4 a sample of check list for evaluation which the result will be only 0 or 1.

4. What is the percentage of employees who have read and signed the Security Policy?
Derived from the second metric, the policy to be effective, it has to be known and accepted by the users of the system.
Method: Scorecard
Evaluation: [(Number of Employees signed the policy) / (Total number of employees)] *100

Figure 2.5 Example evaluation method

Figure 2.5 a sample of evaluation which result represent in percentage. This work will use point from check list or result of evaluation to measuring performance ICT Security in organization.

Chenxi Wang and William A. Wulf [2] developed security measurement framework of computer security used Analytic Hierarchy Process (AHP) to help identify the relative importance among sibling components. Calculation score used Weakest Link (WL), Weighted Weakest Link (WWL) and Prioritized Siblings (PS).

	Job	Study	Personal	Social	weights using λ_{max}
Job	1	1/2	4	5	0.324
Study	2	1	5	6	0.508
Personal	½	1/5	1	2	0.103
Social	1/5	1/6	1/2	1	0.066

Figure 2.6 Example result of pair-wise comparisons

Figure 2.6 they use an example to illustrate the AHP weight judgment method. A student wants to determine the relative importance of four activities in his life: A part-time job, study, personal activities and social activities. Using AHP, he will first make six pair-wise comparisons according to a pre-defined scale. The results of the comparisons are shown in a matrix.

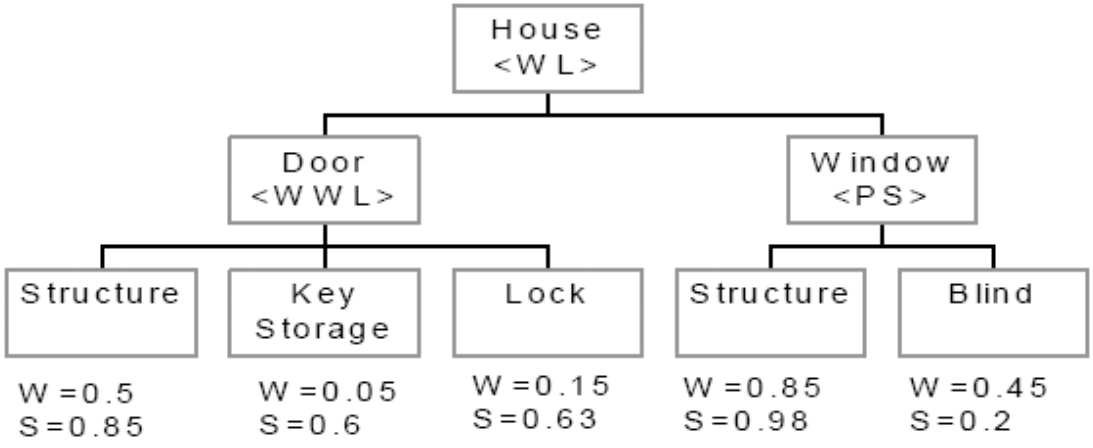

Figure 2.7 Example decomposition tree for house

Figure 2.7 shows example decomposition tree of house system. Define weight and score of child node.

2.3 Objectives

This research aims to accomplish the following objectives.

1. To study the possibility of ICT security evaluation in organization.
2. To study evaluation method of ICT security in organization.
3. To study how to use balanced scorecard in ICT security evaluation.
4. Apply scorecard to represent the consequence of ICT security evaluation.
5. Develop a prototype system of ICT security evaluation in organization using the concept of balance scorecard for displaying results.

2.4 Scope of the work

We intend to design and develop a prototype system with the following features:

1. ICT security evaluation system can be divided into main 11 perspectives. For each perspective include to objective and measure.
2. A prototype system able to calculate weight from the way to setup priority of component.
3. A prototype system able to calculate score of component and branch.
4. A prototype system able to calculate total score of province, region and organization.
5. A prototype system able to create boundary to represented scorecard in 3 colors are red, yellow and green.
6. A prototype system able to represent the result of ICT security evaluation in tree and table format.
7. A prototype system able to represent the result of ICT security evaluation in scorecard for branch, province, region and organization.

CHAPTER III
CONCEPTUAL DESIGN

3.1 Organization case study

In this research project, the development of the prototype to measure the efficiency of the ICT security within an organization aims to investigate a Thai bank's structure as a case study. Typically, local banks will expand their branches to provinces and districts across the country, which make them have a variety of locations (areas) and environments. As a result, the measurement of the ICT security efficiency for each branch of a bank generally differs. It is worth noting that a bank's operation tends to decentralize its authority, duties and responsibilities to its branches in the regions, provinces and districts throughout the country. The structure of a bank's organization is revealed in Figure 3.1.

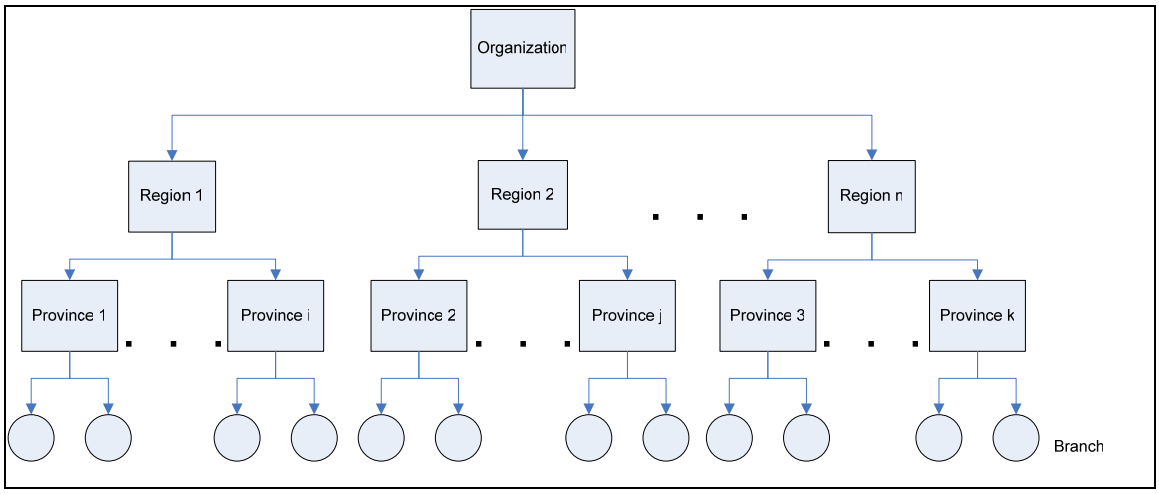

Figure 3.1 Organization structure

Based on Figure 3.1, a bank's organizational structure consists of 4 levels of organization listed below.

- Organization is an organizational level, composed of different region.
- Region is a regional level, with various regional centers (RC) serving as hubs controlling a communicative that of branches under its jurisdiction.
- Province is a provincial level, consisting of different branches.
- Branch is a branch level, comprising branches of the headquarters, and micro branches in a number of districts and provinces.

For a measurement of the ICT security efficiency within the organization, the efficiency of each bank's branch will be measured and the overall consequences are concluded as a measurement result at provincial, regional and organizational levels.

3.2 Model

A measurement of the ICT security efficiency is made on several components of security, which interact with on another, to ensure an efficient consequence.

3.2.1 Component

A component is an element of a measurement of the ICT security efficiency by compiling from the international standard for ICT safeguarding (ISO/IEC 17799). The security components are classified into 11 components as the following:

1. Security policy
2. Physical security
3. Facility security
4. Personnel security
5. Hardware security
6. Software security
7. Data security
8. Network security
9. Regulatory security

10. Contingency planning and disaster recovery
11. Incident reporting

ICT security policy It is the formulation of policies and the laying of foundation of the ICT security maintenance in order to strengthen an organization's ICT infrastructure and become the basis in support of its business transactions.

Physical security It is an arrangement of a proper place for an ICT operation to prevent an access of threat to a room for the computer system.

Facility security It is an arrangement of such facilities as the power system, communicative system, air-conditioning system, fire prevention system, and alarming system, to ensure an organization's perfect, continuous and smooth performance.

Personnel security It is a determination of the management guideline to reduce operational risks that may arise from human error, an insufficient internal control system that may result in corruption, or misuse of ICT equipment.

Hardware security It is a proposal of an operational guideline for generating an organization' equipment security, concentrating on hardware planning, equipment access control, including adequate equipment reservation.

Software security It is a proposal of an operational guideline for creating confidence in the security of an organization's software, both the system software and applied operating system software, a serious control of operating system access with a password, a systematic enforcement of the password, and a prevention of software derogatory to the operating system.

Data security It is a proposal of a guideline for the management of an organization's data storage and ICT, covering data classification, data reservation, management of data recording media, control of data usage, and data elimination.

Network security It is a proposal of a management guideline covering the planning for an efficient communicative network system, security of such network equipment as LAN switch, router, modem , etc, defining network addressing and naming to correspond to international standard, control of linkage and access to the communicative network system, as well as protection of the system from an attack by perilous software.

Regulatory security It is a proposal of an operational guideline concerning rules and regulations in order to regulate the performance of staff taking charge of ICT work so that it goes in accordance with an organization's ICT security maintenance guideline.

Contingency planning and disaster recovery It is a proposal of a guideline for coping with an emergency and recovering the system so that it comes back to normal after an emergency. This covers an establishment of the task force in case of an emergency, preparation before an emergency occurs, dealing with an emergency and evaluating the damage incurred, including a guideline for recovering the system until it is normalized so that an organization's business transaction can be consistently performed.

Incident reporting It is a proposal of a guideline for recording data on incidents regarding ICT into a computer system, whether the incidents are normal or not. This aims to be the information for reporting incidents that may arise to the people concerned so that they can resolve the problem immediately. The workflow of the report, including the data in the system, will be made into a summary report to be presented to the executives for use in decision-making and giving an order for a further implementation.

The 11 major components discussed above are divided into sub-components to broaden the coverage of measurement and increase measurement efficiency. In this research project, components are classified into 3 levels as follows:

- Perspective is all the 11 major component.
- Objective is the objective of each perspective.
- Measure is the indicator of each objective.

3.2.2 Interaction

Components used to measure the ICT security efficiency generally interact with one another in the pattern of parent-child, with the following details.

1. Interaction of component

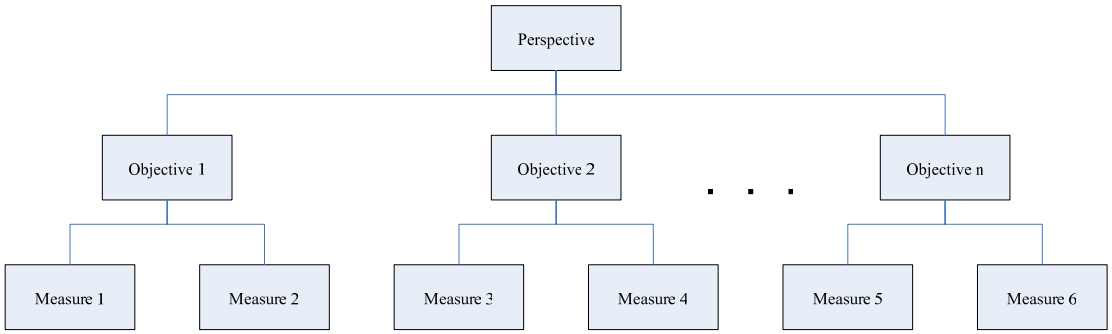

Figure 3.2 Model of component

Figure 3.2 The structure of components used to measure the ICT security efficiency consists of the following.

- Perspective interacts with the objective which is the child of that perspective.
- Objective interacts with the perspective which is the parent, and will measure only the child.
- Measure interacts with the objective which is the parent

2. Interaction of branch

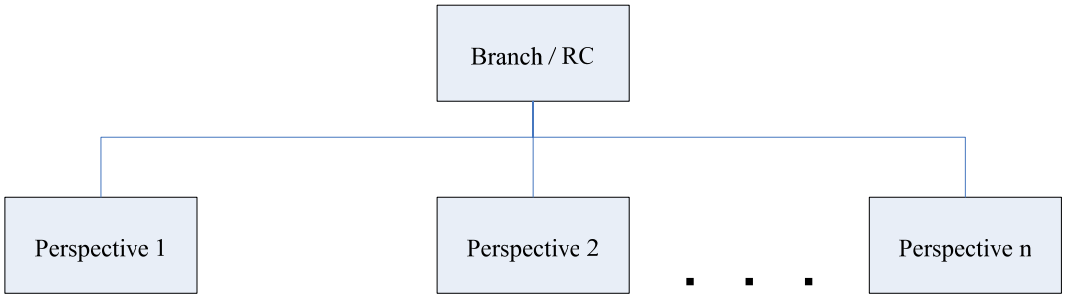

Figure 3.3 Model of branch

Figure 3.3 The structure of branch used to measure the ICT security efficiency consists of the following.

- Branch / RC interacts with the perspective which is the child of branches or regional centers only.
- Perspective interacts with the objective which is the child of that perspective.

3. Interaction of province

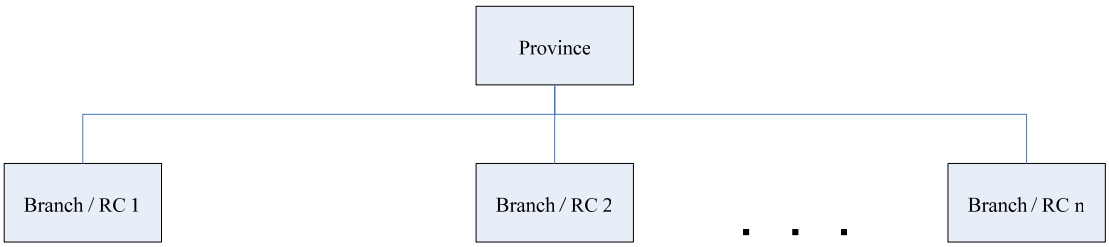

Figure 3.4 Model of province

Figure 3.4 The structure of province used to measure the ICT security efficiency consists of the following.

- Province interacts with the branch or regional center concerned.

- Branch / RC interacts with the perspective which is the child of branches or regional centers only.

4. Interaction of region

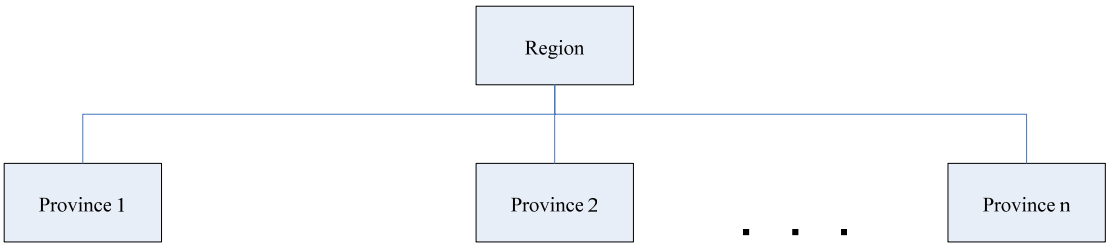

Figure 3.5 Model of region

Figure 3.5 The structure of region used to measure the ICT security efficiency consists of the following.

- Region interacts with the province concerned.
- Province interacts with the branch or regional center concerned.

5. Interaction of organization

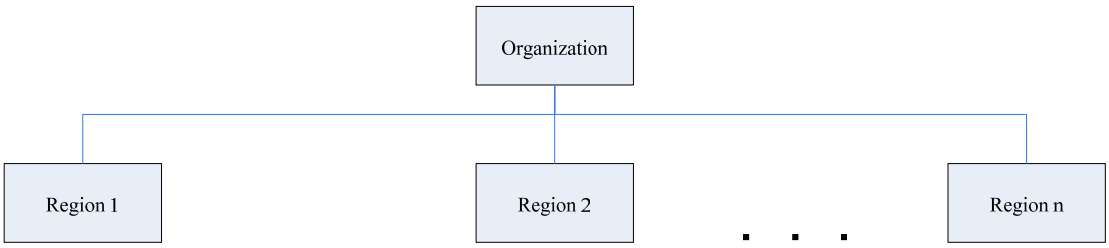

Figure 3.6 Model of organization

Figure 3.6 The structure of organization used to measure the ICT security efficiency consists of the following.

- Organization interacts with the region concerned.
- Region interacts with the province concerned.

3.3 Calculation method

To measure the ICT security efficiency, all the components used to measure have to be evaluated by calculating their weight and score. Calculation details are described below.

3.3.1 Calculation of weight

Since weight is a variable used to measure the ICT security efficiency, the weight of each component will be defined. This means the prioritization of components, which is different for each bank's branch, depending on the prioritization and environment of each branch. For prioritization, it is different opinions of each person. In this project, each level of components has various standards for measurement. Thus, a method of analytic hierarchy process (AHP) is used to prioritize components used to measure because AHP is a multi-measure analytic approach, which is a pairwise comparison of components. The comparison is a transformation of qualitative measurement into a scale so that a qualitative evaluation can be made, as revealed in Table 3.1

ระดับความสำคัญ หรือความชอบ (Preference Level)	ค่าแสดงเป็นตัวเลข (Numerical Valve)
เ ท่ากัน (Equally Preferred)	1
เท่ากันถึงปานกลาง (Equally to Moderately Preferred)	2
ปานกลาง (Moderately Preferred)	3
ปานกลางถึงค่อนข้างมาก (Moderately to Strongly Preferred)	4
ค่อนข้างมาก (Strongly Preferred)	5
ค่อนข้างมากถึงมากกว่า (Strongly to Very Strongly Preferred)	6
มากกว่า (Very Strongly Preferred)	7
มากกว่าถึงมากที่สุด (Very Strongly to Extremely Preferred)	8
มากที่สุด (Extremely Preferred)	9

Table 3.1 Preference level

Steps of analysis by an approach of analytic hierarchy process (AHP)

An analysis via the AHP method is used to calculate the weight of components used to measure. In this regard, the priority value of components will be computed to get their weight. Computation steps are described below.

1. Each level of components is analyzed through a pairwise comparison and priority value determination of components, based on Table 3.1

Where a_{ij} is priority value derived from a pairwise comparison at the same level, in the case that component I is more significant than component j; and $1 / a_{ij}$ is an inverse significant value, in the case that component j is more significant than component i.

$$\begin{bmatrix} a_{11} & a_{1n} \\ a_{21} & \\ & \\ a_{n1} & a_{nn} \end{bmatrix}$$

We define the prioritization value as follows:

- If i = j then $a_{ij} = 1$
- If i > j then $a_{ij} = 1 / a_{ji}$
- If i < j then a_{ij} = pairwise comparison value

2. To normalize the weights, compute the sum of each column and then divide each column by the corresponding sum.

$$\begin{bmatrix} \delta_{11} = a_{11} \Big/ \sum_{i=1}^{n} a_{i1} & \delta_{1n} = a_{1n} \Big/ \sum_{i=1}^{n} a_{in} \\ \\ \delta_{n1} = a_{n1} \Big/ \sum_{i=1}^{n} a_{i1} & \delta_{nn} = a_{nn} \Big/ \sum_{i=1}^{n} a_{in} \end{bmatrix}$$

3. To compute the sum of each row.

$$\begin{bmatrix} \beta_1 = \sum_{j=1}^{n} \delta_{1j} \\ \beta_2 = \sum_{j=1}^{n} \delta_{2j} \\ \\ \beta_n = \sum_{j=1}^{n} \delta_{nj} \end{bmatrix}$$

4. The next step is to compute the average values of each row and use these as the weights in the component hierarchy. Note that by construction, summation of weight equal to 1.

$$\begin{bmatrix} r_1 = \frac{\beta_1}{n} \\ r_2 = \frac{\beta_2}{n} \\ \\ r_n = \frac{\beta_n}{n} \end{bmatrix}$$

3.3.2 Calculation of score

The score is a variable used to measure the ICT security efficiency. The determination of score of each bank's thus differs based on its environment and actual situation. To measure the efficiency of each branch, only the measure level will be evaluated. For other levels, the system will calculate the value based on the detail which will be further discussed. In addition, the system also computes total scores of provinces, regions and the organization so that an overall picture of the ICT security within the organization can be viewed. The score calculation is divided into 2 part, namely, that of branches and that of provinces, regions and the organization, all in total.

3.3.2.1 Calculation of branch score

A calculation of scores based on the evaluation of each branch is divided into 2 methods: calculation of measure scores, and calculation of parent scores.

1. Measure level

The determination of scores at the measure level is derived from an evaluation of users, with the scores in each measure being between 0 and 100.

2. Parent level

The determination of scores at the objective, perspective and branch levels is obtained from calculating the score of child with the weight of child since the significance of each component is defined, and thus the weight is also computed. It can be explained in the following form of formula.

$$S(Parent) = \sum_{i=1}^{n} \frac{(S(Child_i) \times W(Child_i))}{100}$$

i = Child node

n = Number of child node under the parent

S(Parent) = Parent score

S(Child) = Child score

W(Child) = Child weight

3.3.2.2 Calculation of summary score

A calculation of summary scores of provinces, regions and the organization is divided into 2 parts, namely, calculation of component scores of provinces, regions and the organization, and that of average score of provinces, regions and the organization.

1. Component score

To calculate component scores, the average score of perspective, objective and measure are computed for each branch concerned (under supervision), which is divided into 2 following methods.

- Measure level

To calculate measure scores, the average measure score of all child nodes under supervision is computed using the above formula.

$$S(M_{Parent}) = Avg(S(M_{Child_1}), S(M_{Child_2}), ..., S(M_{Child_n}))$$

$S(M_{Parent})$ = Measure score of parent

$S(M_{Child})$ = Measure score of child

n = Number of child node under the parent

- Objective and perspective level

To calculate scores of objective and perspective, the average score of child nodes under parent is computed based on the above formula.

$$S(Parent) = Avg(S(Child_1), S(Child_2), ..., S(Child_n))$$

$S(Parent)$ = Parent score

$S(Child)$ = Child score

n = Number of child node under the parent

2. Summary score

To calculate summary scores of provinces, regions and the organization, the average score of child nodes under parent is computed, with the following detail.

- To calculate province scores, the average score of all branches under the supervision of that province is computed.
- To calculate region scores, the average score of all provinces under the supervision of that region is computed.
- To calculate organization scores, the average score of all regions is computed.

$$S(Parent) = Avg(S(Child_1), S(Child_2), ..., S(Child_n))$$

$S(Parent)$ = Parent score

$S(Child)$ = Child score

n = Number of child node under the parent

3.4 Example scorecard

It is a display of an example of the consequence of ICT security efficiency measurement, in the form of a scorecard using colors for the presentation. In this connection, the most recent outcome of ICT security efficiency measurement of each branch is displayed so that the current status of ICT security inside the organization can be observed. The scorecard is revealed in 2 forms of tree and table.

1. Tree scorecard

A display of an example of the outcome of ICT security efficiency measurement in the form of tree is divided into 4 levels, with the derived score displayed in color.

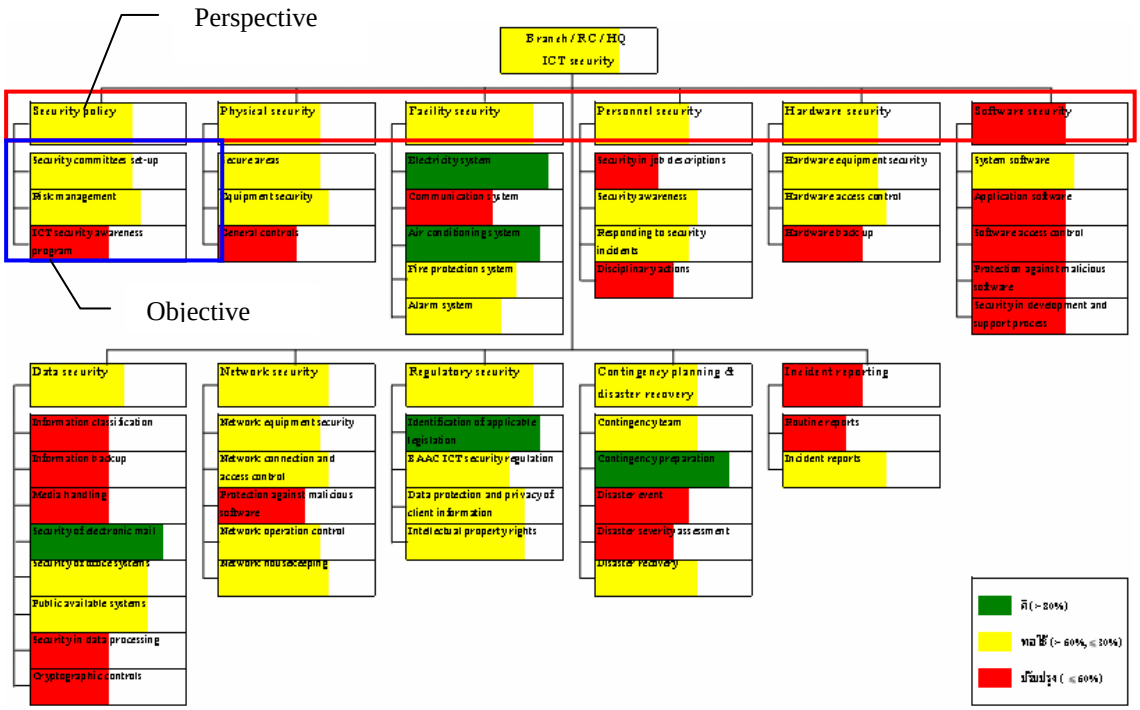

Figure 3.7 Example scorecard in tree form

Figure 3.7 The details are discussed below.

- Level 1: Branch/RC/HQ is a display of the result of ICT security efficiency measurement of branches, regional centers, and headquarter' branches. The scores are obtained from a score calculation of different perspectives.

- Level 2: Perspective is a display of the outcome of ICT security efficiency measurement of all 11 perspectives. The scores are derived from a score calculation of objectives under these perspectives.

- Level 3: Objective is a display of the consequence of ICT security efficiency measurement of objectives. The scores are received from a score calculation of measures under these objectives.

- Level 4: Measure is a display of the result of ICT security efficiency measurement of measures, following the objective level. The scores are obtained from an assessment by evaluators.

2. Table scorecard

A display of an example of the outcome of ICT security efficiency measurement in the form of table is classified into 5 major columns.

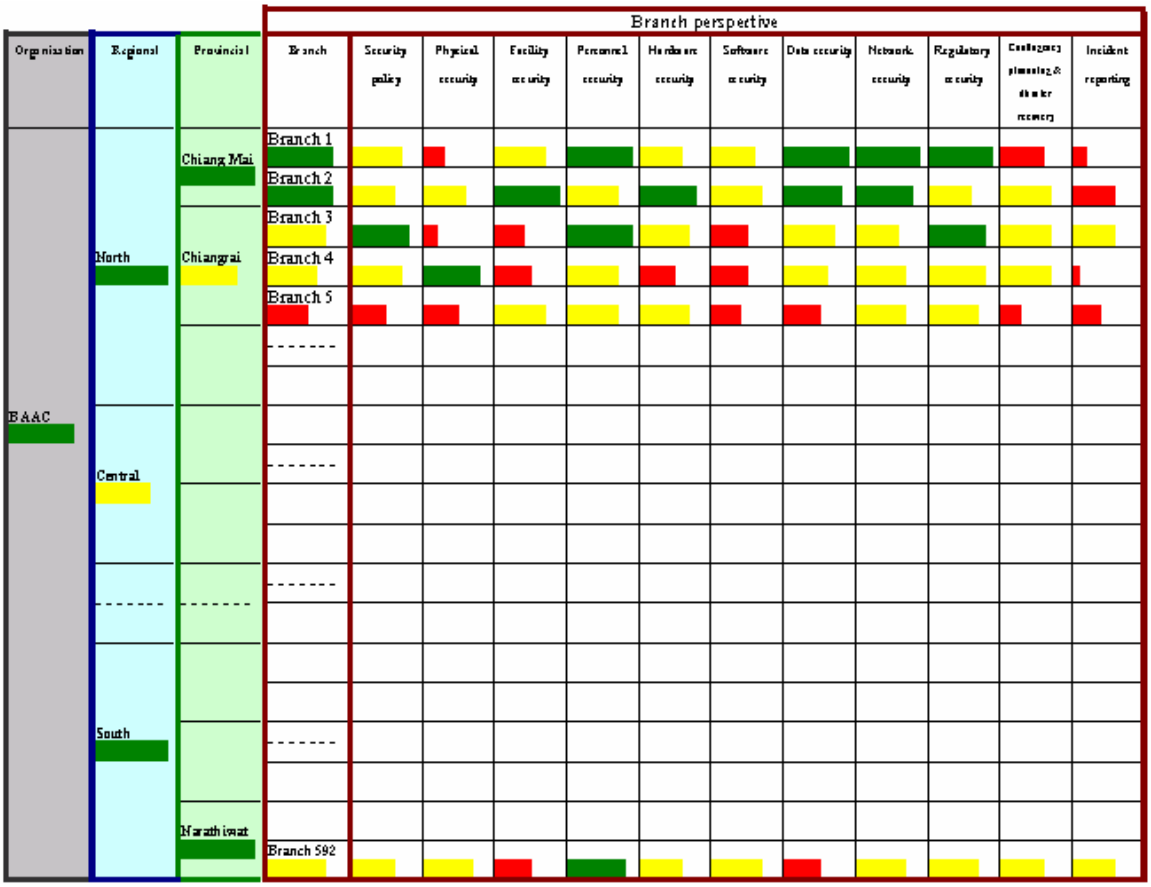

Figure 3.8 Example scorecard in table form

Figure 3.8 The details described below.

- Column 1: Organization is a display of the result of ICT security efficiency measurement of the organization. The average score of different regions is calculated to reveal an overall picture of the organization.

- Column 2: Regional is a display of the outcome of ICT security efficiency measurement of different regions. The average score of provinces under the supervision of each region is calculated to show an overall picture of each region.

- Column 3: Provincial is a display of the consequence of ICT security efficiency measurement of different provinces. The average score of branches under the supervision of each province is computed to demonstrate an overall picture of each province.

- Column 4: Branch is a display of the result of ICT security efficiency measurement of branches, regional centers, and the headquarter's branches. The scores of different perspectives used to measure are calculated with the weight of each perspective to get the total scores of each branch.

- Column 5: Branch perspective is a display of the outcome of the ICT security efficiency measurement of different perspectives in each branch. The scores of various objectives used to measure under these perspectives are computed with the weight of each objective to gain the total scores of perspectives.

CHAPTER IV
DETAILED DESIGN

This chapter describes use case diagrams, class diagrams, sequence diagrams, file structure and module specification.

4.1 Use case diagrams

Use case diagrams represent the functionality of the system from a user's point of view. Actors are external entities that interact with the system. Use cases describe the behavior of the system as seen from an actor's point of view.

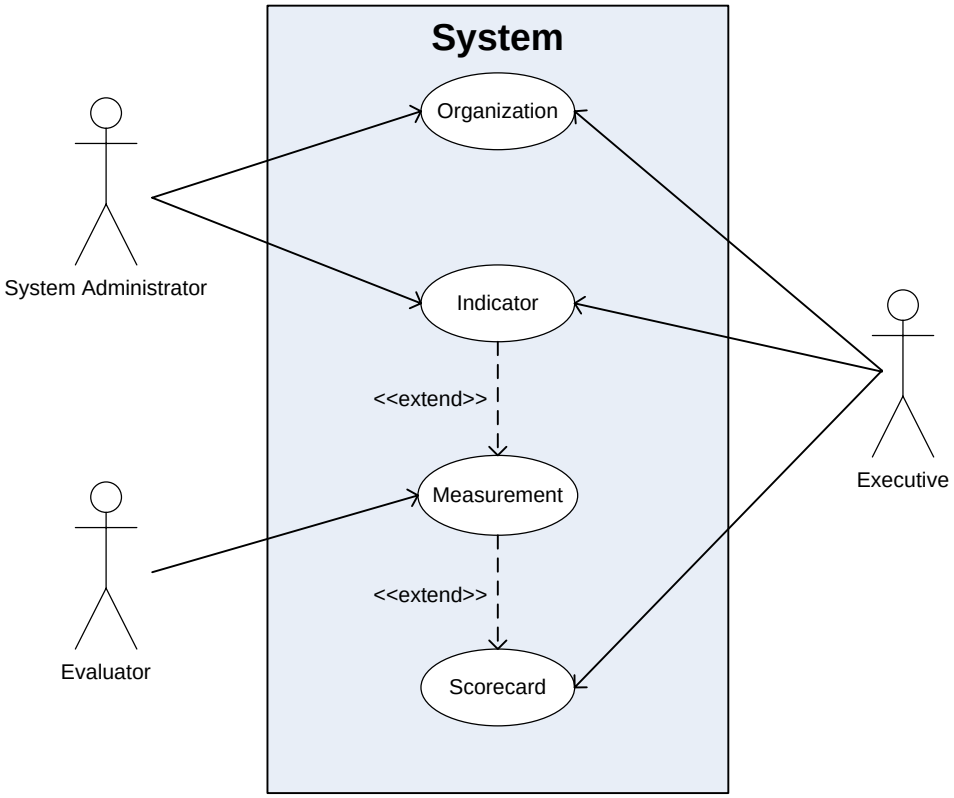

Figure 4.1 Use case diagram for system

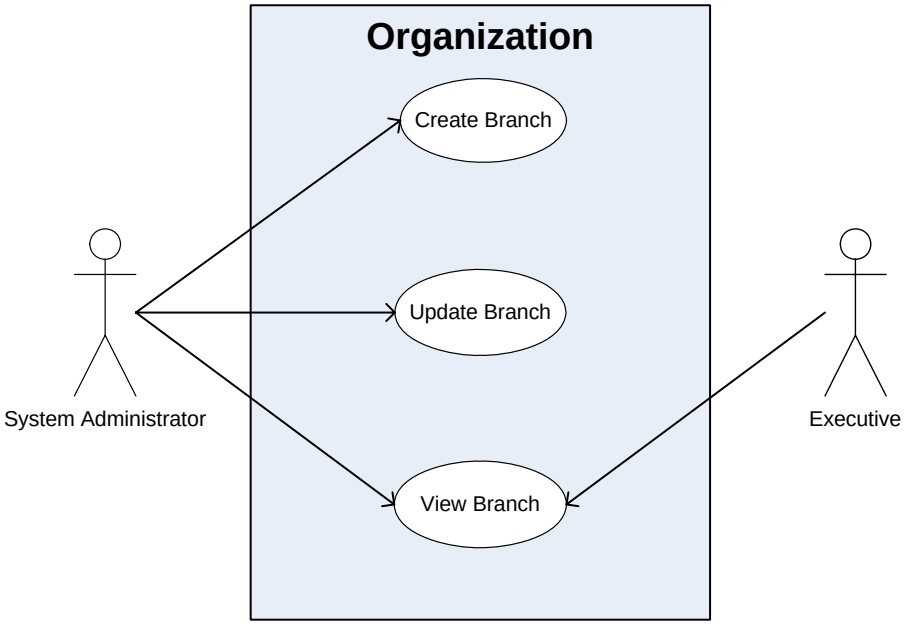

Figure 4.2 Use case diagram for organization

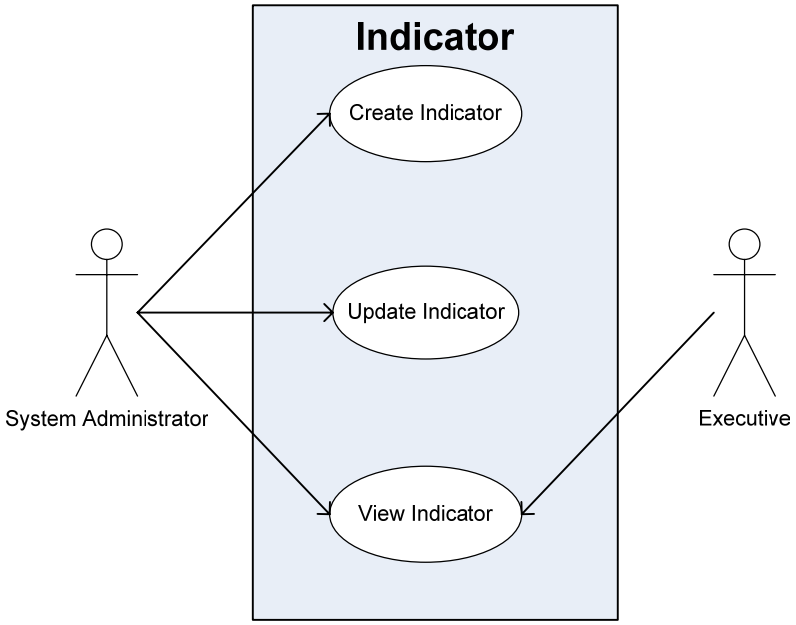

Figure 4.3 Use case diagram for indicator

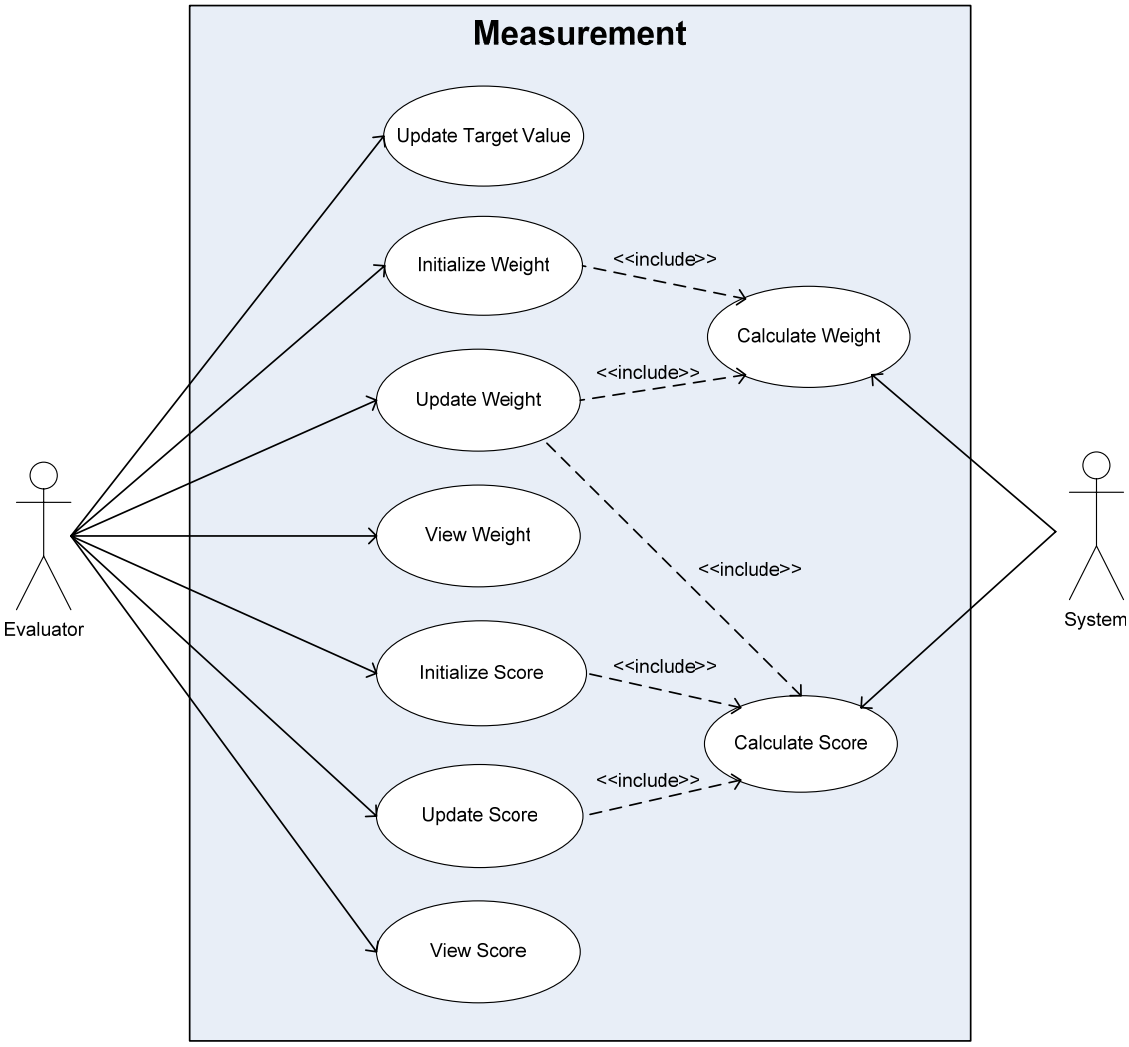

Figure 4.4 Use case diagram for measurement

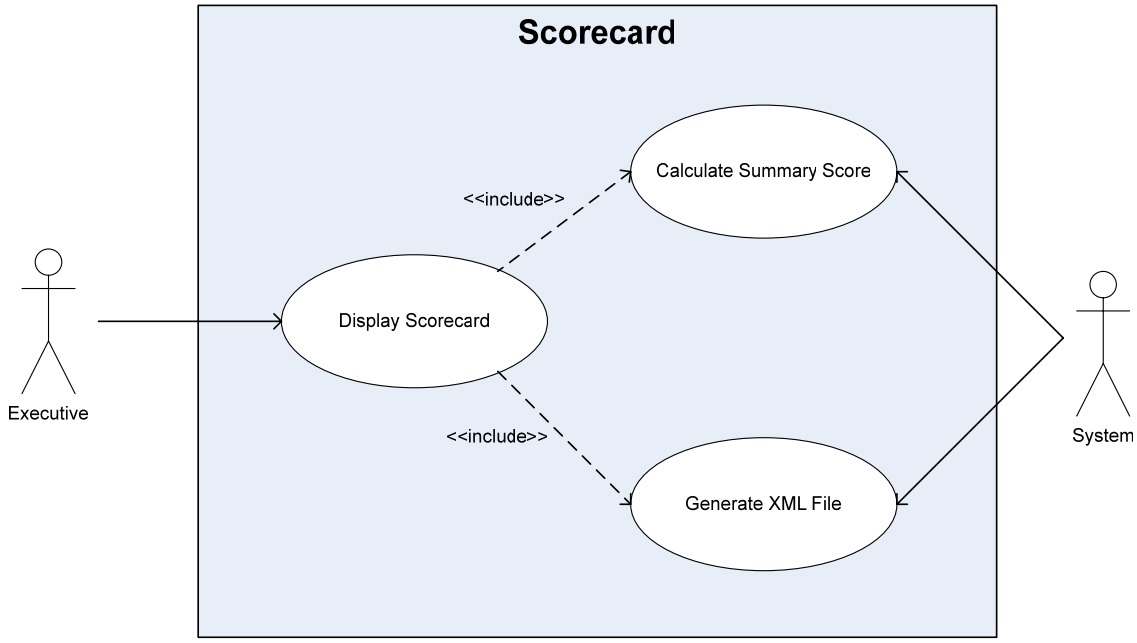

Figure 4.5 Use case diagram for scorecard

Use case name	Create branch
Participating actors	System administrator
Flow of events	1.System administrator request create new branch. 2.Organization responds by presenting a create form to the system administrator. 3.System administrator input branch information to create form. 4.Organization verify branch information if branch is exist then reject else save branch information to database

Use case name	Update branch
Participating actors	System administrator
Flow of events	1.System administrator request update branch. 2.Organization responds by presenting a update form to the system administrator. 3.System administrator input branch information to update form. 4.Organization verifies and save branch information to database.

Use case name	View branch
Participating actors	System administrator, executive
Flow of events	1.System administrator or executive search branch. 2.Organization responds by presenting list of branch. 3.System administrator or executive select branch. 4.Organization display branch information.

Use case name	Create indicator
Participating actors	System administrator
Flow of events	1.System administrator request create new indicator. 2.Indicator responds by presenting a create form to the system administrator. 3.System administrator input indicator information to create form. 4.Indicator verify indicator information if indicator is exist then reject else save indicator information to database

Use case name	Update indicator
Participating actors	System Administrator
Flow of events	1.System administrator request update indicator. 2.Indicator responds by presenting a update form to the system administrator. 3.System administrator input indicator information to update form. 4.Indicator verifies and save indicator information to database.

Use case name	View indicator
Participating actors	System administrator, executive
Flow of events	1.System administrator or executive search indicator. 2.Indicator responds by presenting list of indicator. 3.System administrator or executive select indicator. 4.Indicator display indicator information.

Use case name	Update target value
Participating actors	Evaluator
Flow of events	1.Evaluator request update target value. 2.Measurement responds by presenting a update form to the evaluator. 3.Evaluator input target value to update form. 4.Measurement verifies and save target value to database.

Use case name	Initialize weight
Participating actors	Evaluator, system
Flow of events	1.Evaluator request initialize weight. 2.Measurement responds by presenting a form to the evaluator. 3.Evaluator input priority of indicator to form. 4.System calculates weight and save weight to database.

Use case name	Initialize score
Participating actors	Evaluator, system
Flow of events	1.Evaluator request initialize score. 2.Measurement responds by presenting a form to the evaluator. 3.Evaluator input score of indicator to form. 4.System calculates score and save score to database.

Use case name	Update weight
Participating actors	Evaluator, system
Flow of events	1.Evaluator request update weight. 2.Measurement responds by retrieve priority data and presenting to the evaluator. 3.Evaluator input priority of indicator to form. 4.System calculates weight and save weight to database.

Use case name	Update score
Participating actors	Evaluator, system
Flow of events	1.Evaluator request update score. 2.Measurement responds by retrieve score and presenting to the evaluator. 3.Evaluator input score of indicator to form. 4.System calculates score and save score to database.

Use case name	View weight
Participating actors	Evaluator
Flow of events	1.Evaluator request view weight. 2.Measurement responds by retrieve priority data and presenting to the evaluator.

Use case name	View score
Participating actors	Evaluator
Flow of events	1.Evaluator request view score. 2.Measurement responds by retrieve score and presenting to the evaluator.

Use case name	Scorecard
Participating actors	Executive, system
Flow of events	1.Executive request view scorecard. 2.System calculates summary score and generate xml file. 3.Scorecard display scorecard to executive.

4.2 Class diagrams

Class diagrams represent the structure of a system in terms of objects, their attributes, and relationship.

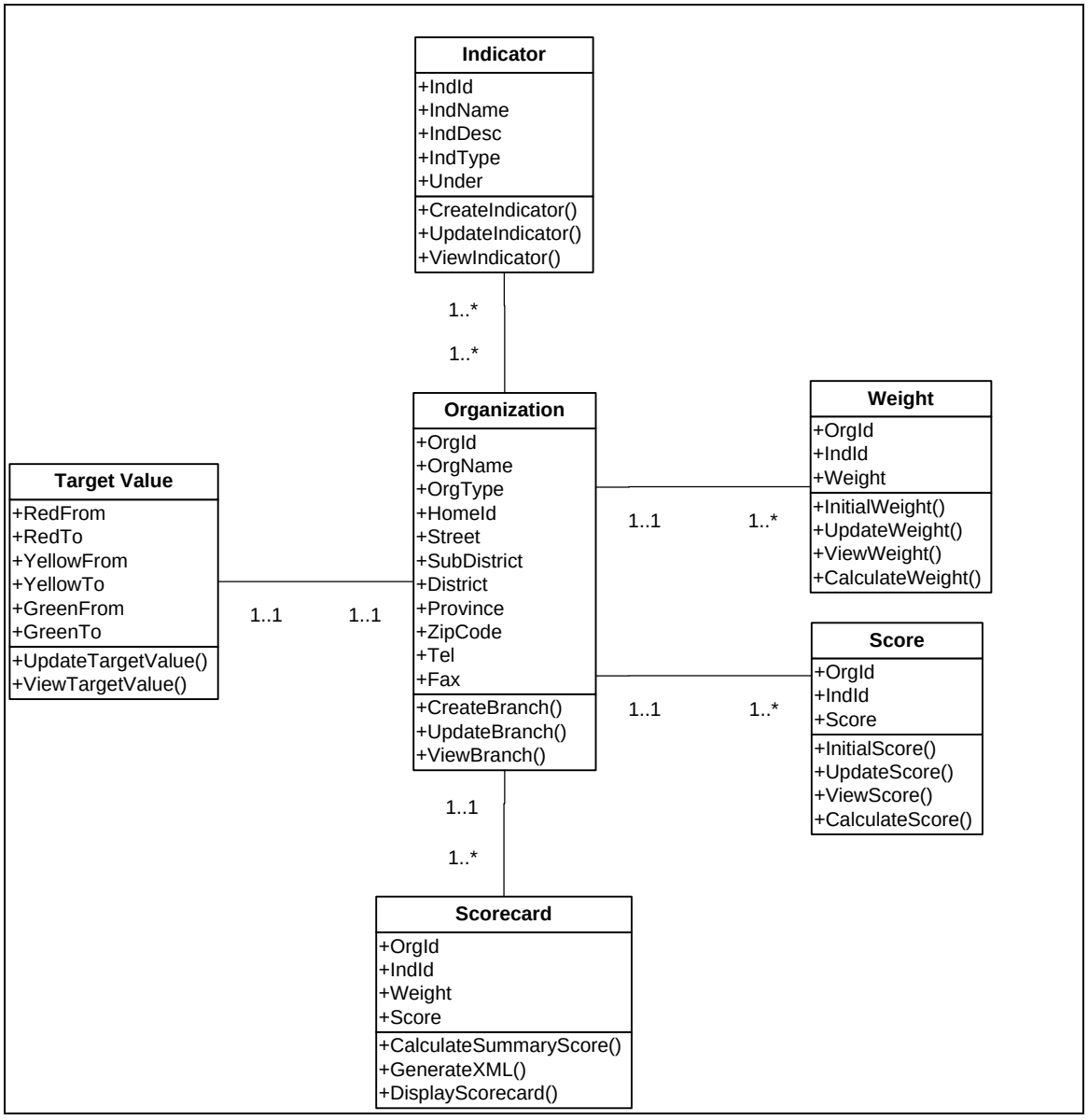

Figure 4.6 Class diagram

Figure 4.6 shown class diagram of a system. Classes are depicted by boxes composed of three compartments. The top compartment displays the name of the class. The center compartment displays its attributes, and the bottom compartment

displays its operations. A link represents a connection between two objects. Associations are relationships between classes and represent groups of links.

4.3 Sequence diagrams

Sequence diagrams represent the objects participating in the interaction horizontally and time vertically.

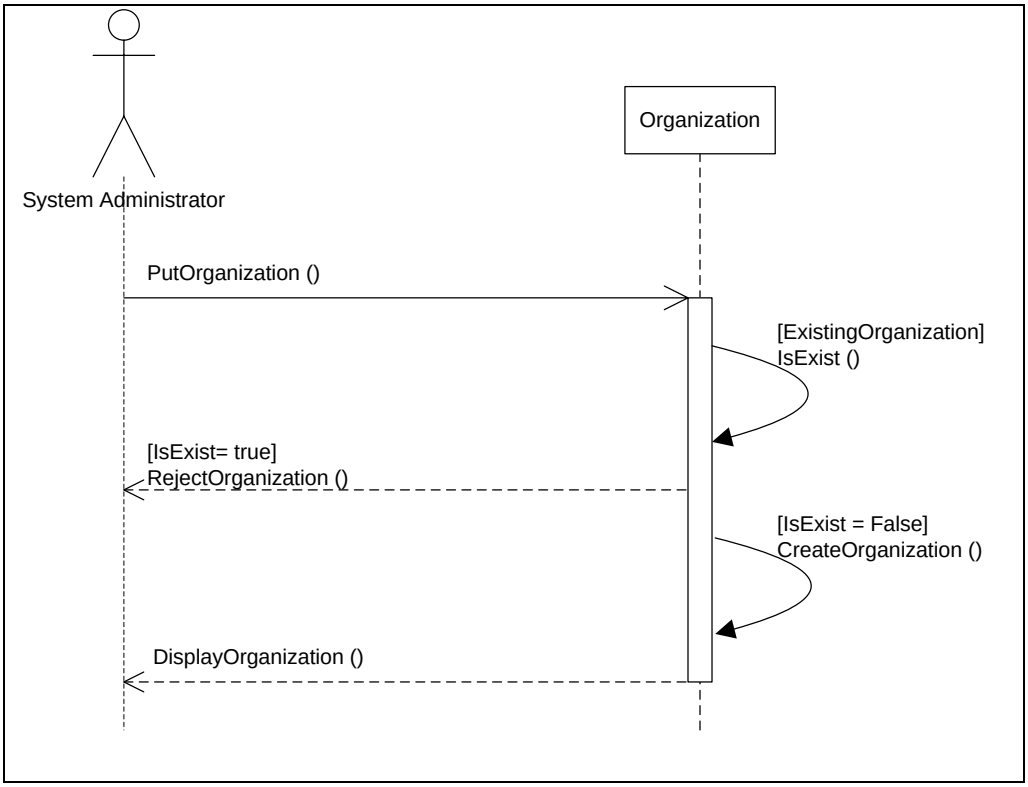

Figure 4.7 Sequence diagram for create branch

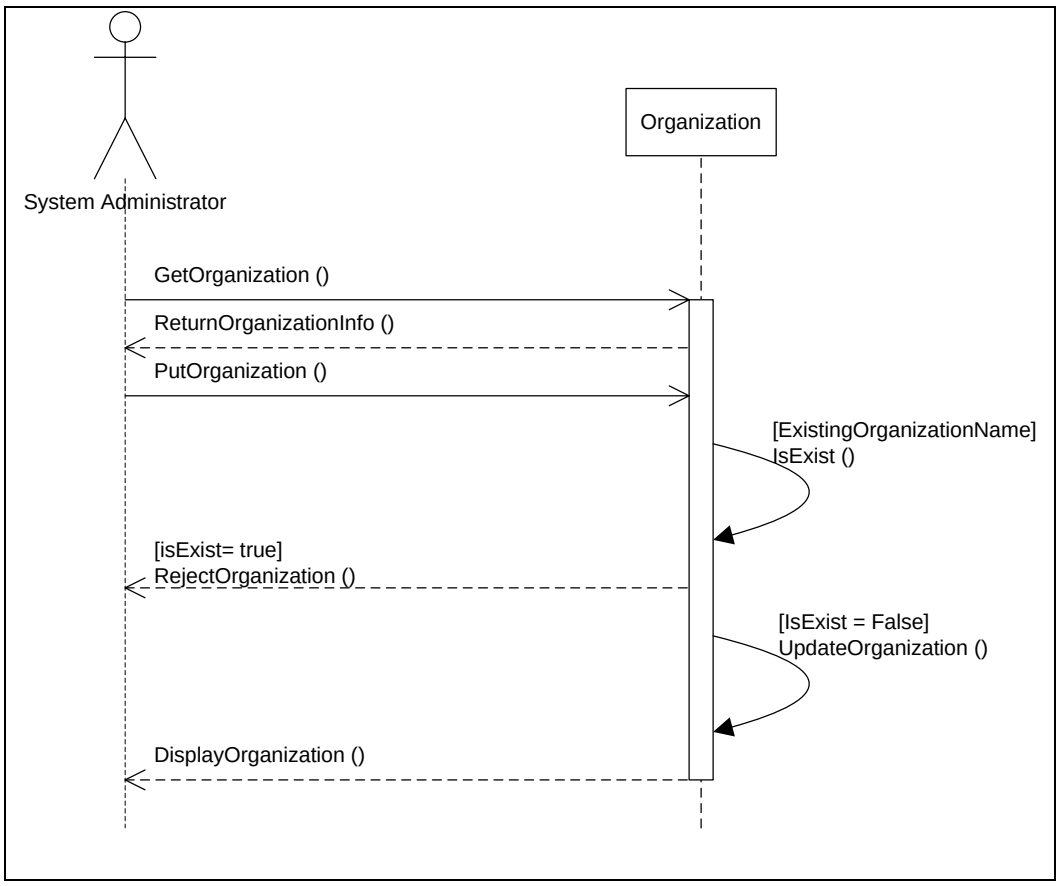

Figure 4.8 Sequence diagram for update branch

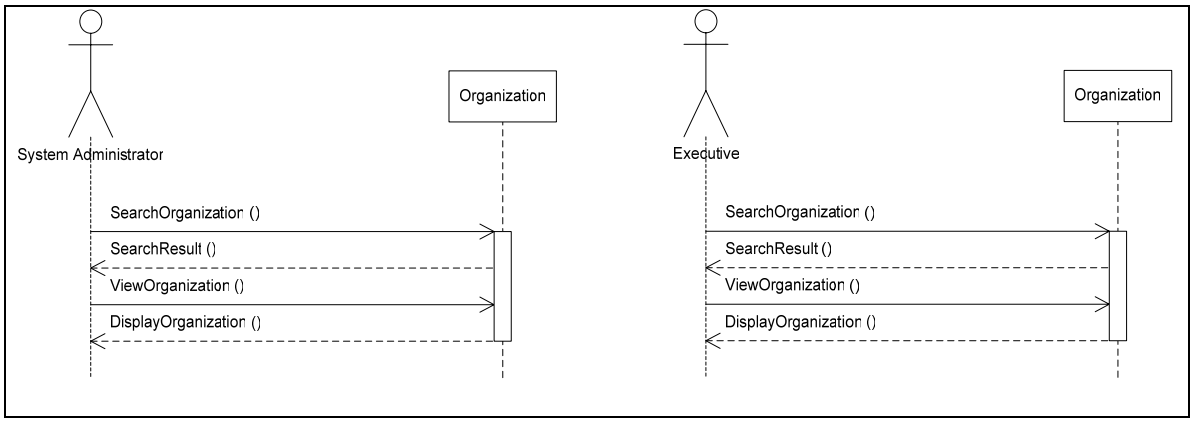

Figure 4.9 Sequence diagram for view branch

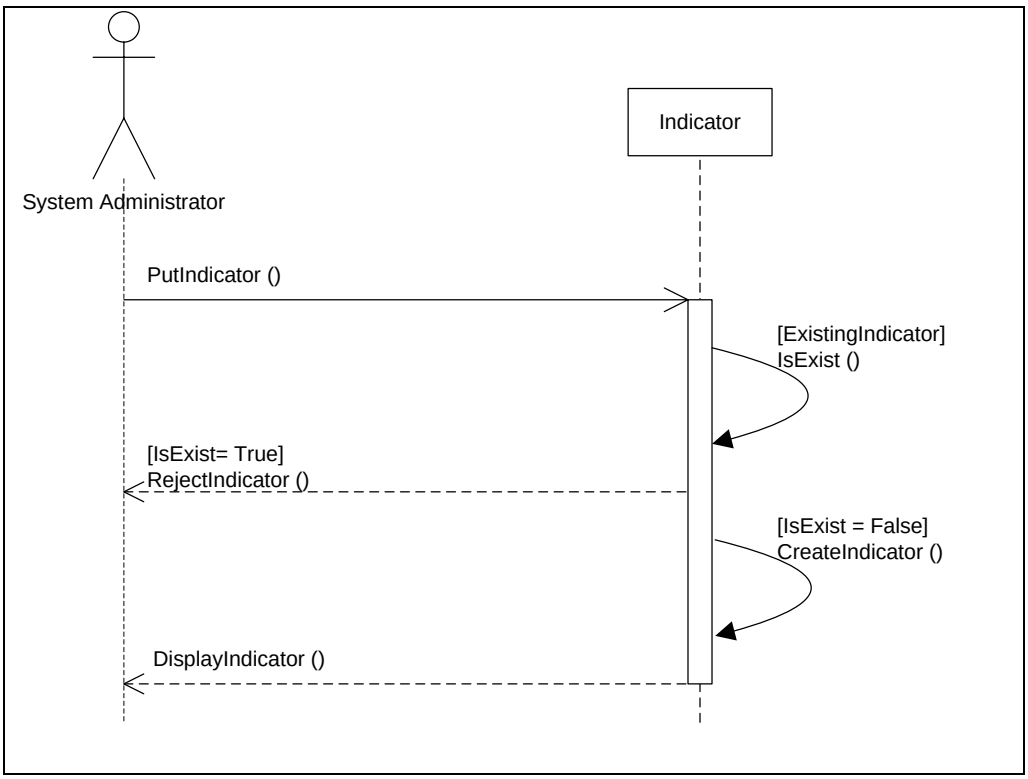

Figure 4.10 Sequence diagram for create indicator

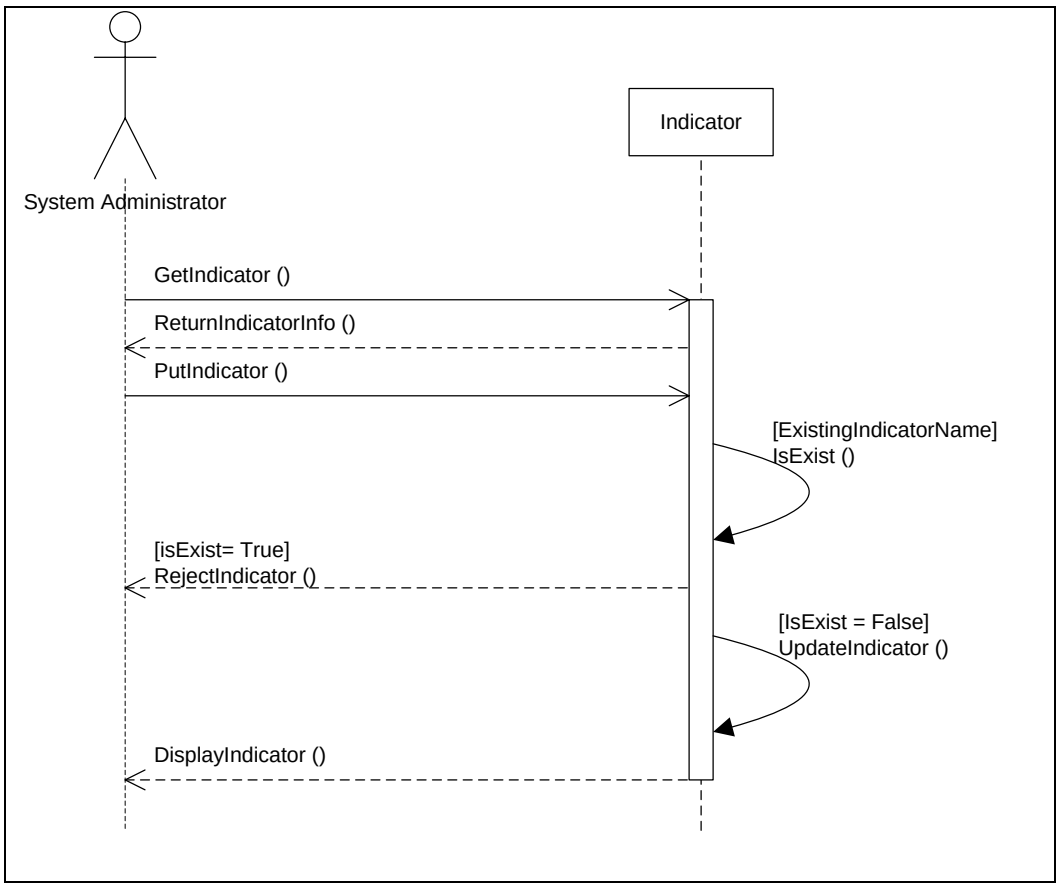

Figure 4.11 Sequence diagram for update indicator

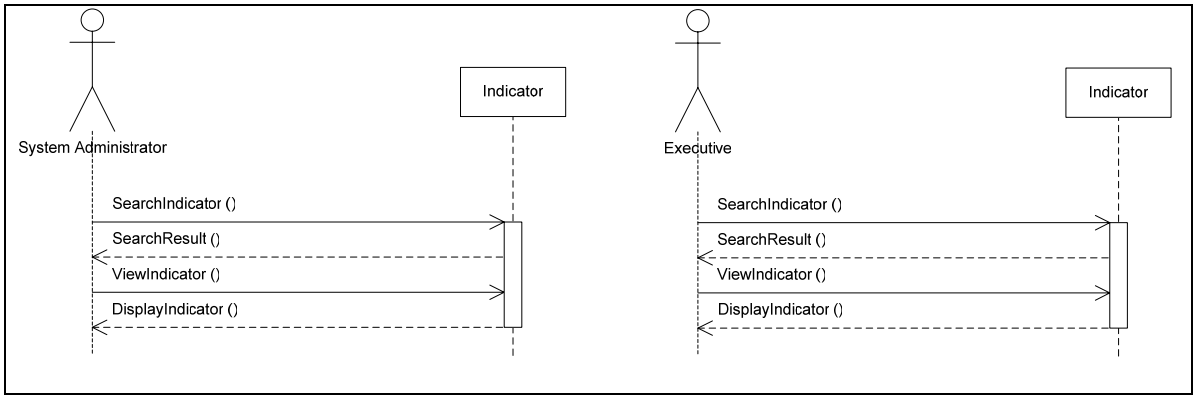

Figure 4.12 Sequence diagram for view indicator

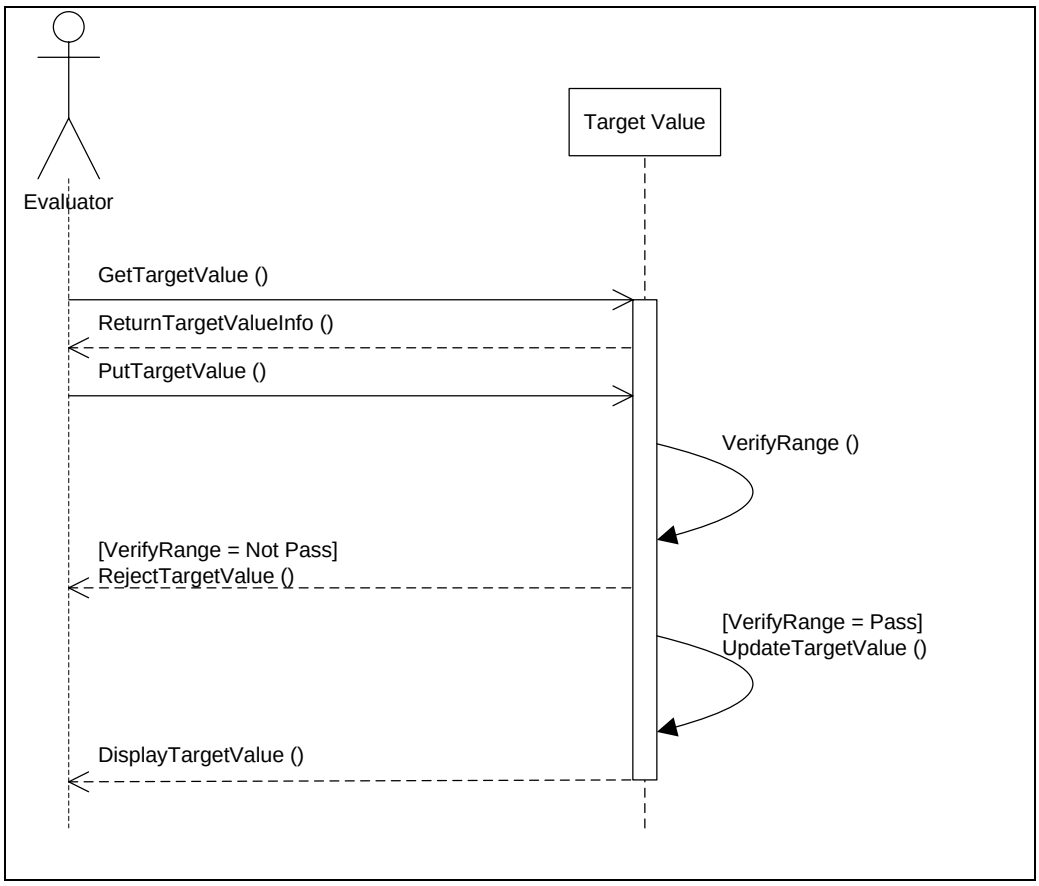

Figure 4.13 Sequence diagram for update target value

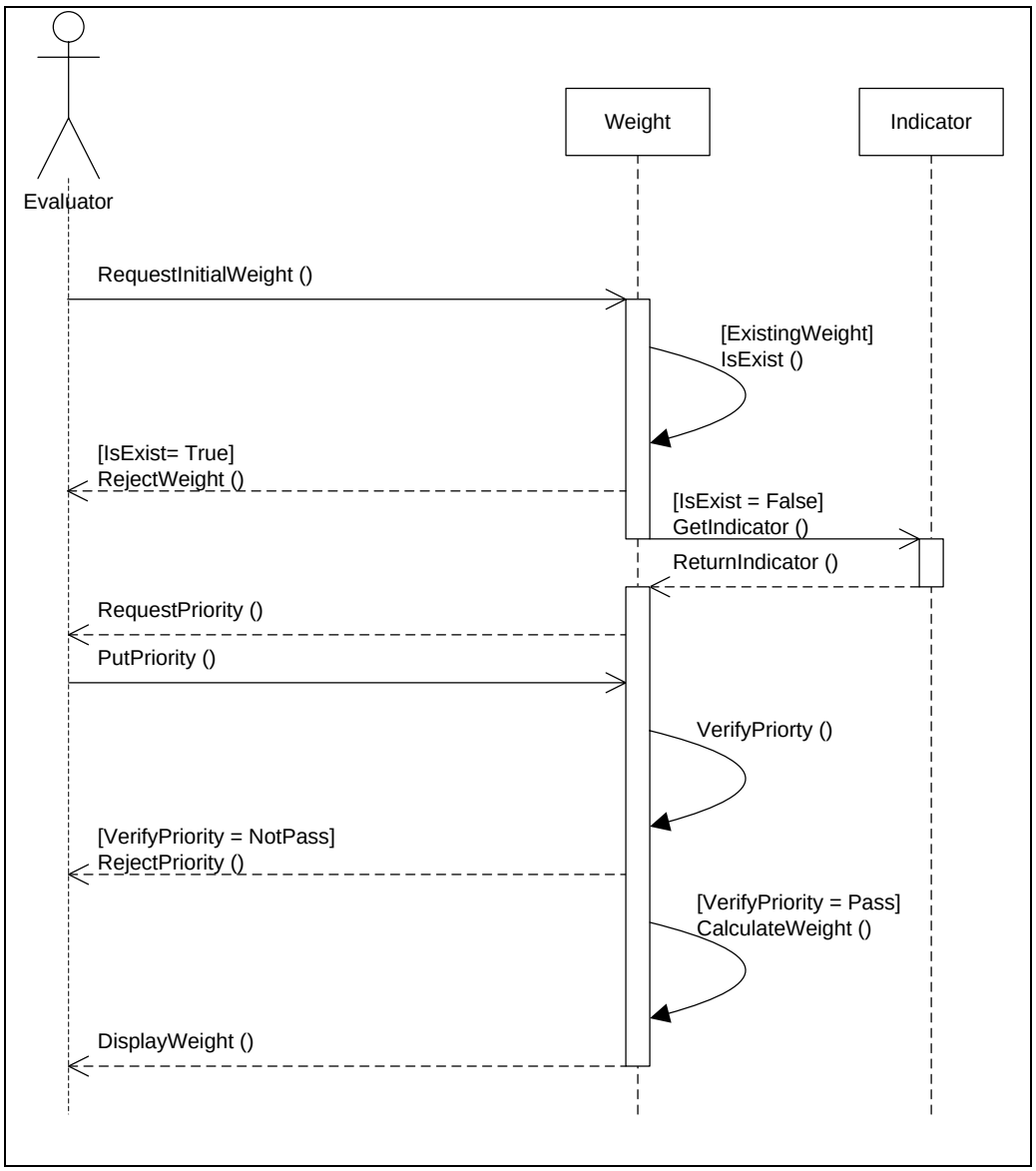

Figure 4.14 Sequence diagram for initialize weight

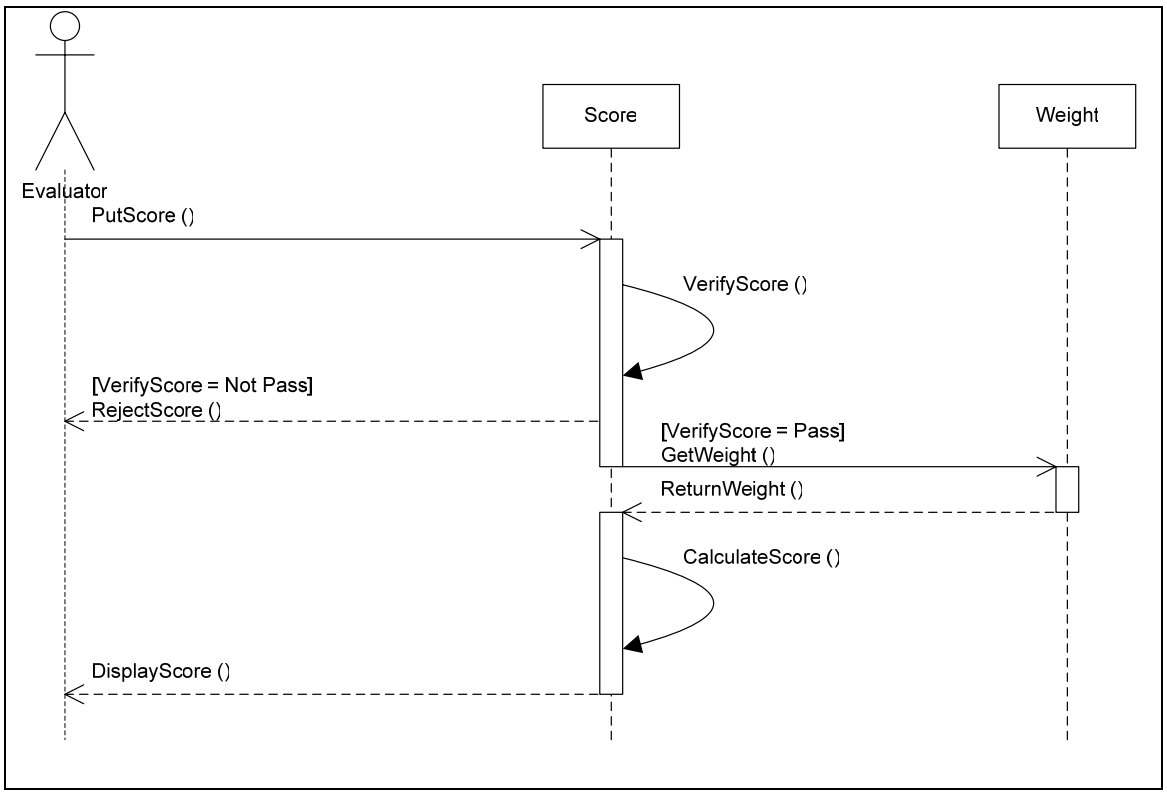

Figure 4.15 Sequence diagram for initialize score

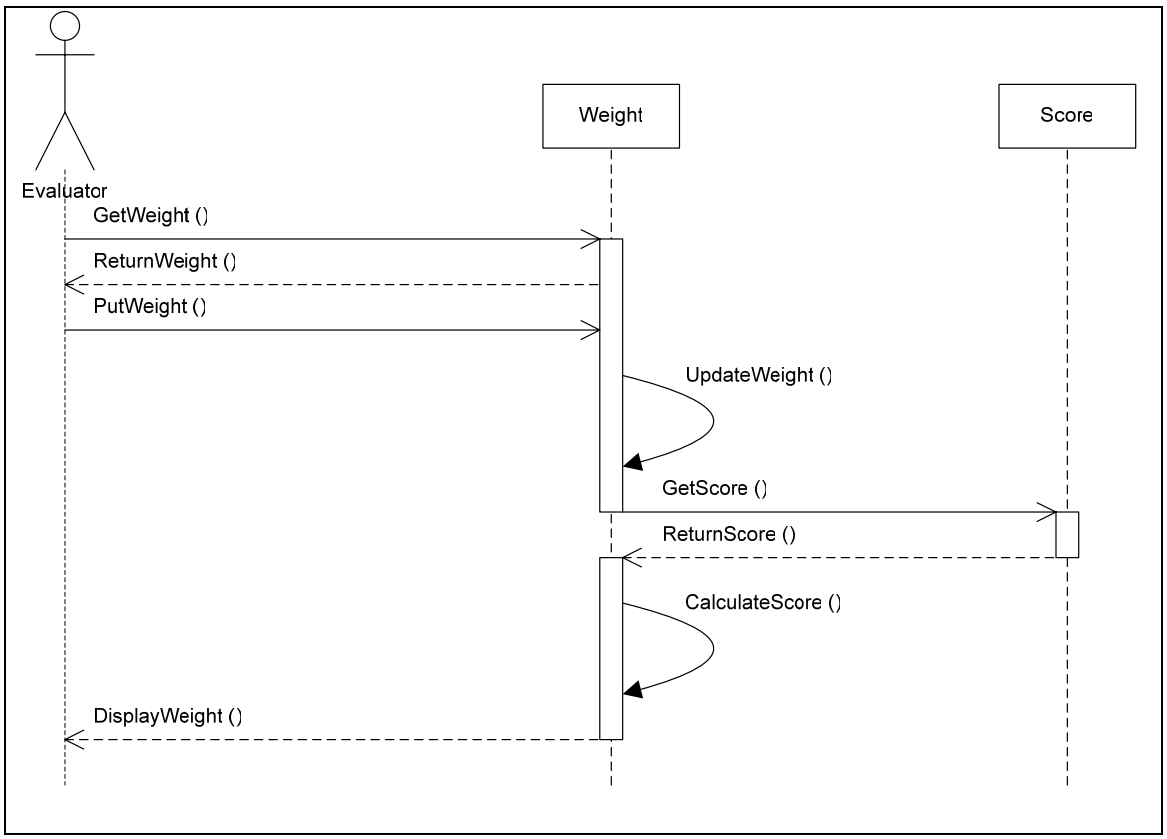

Figure 4.16 Sequence diagram for update weight

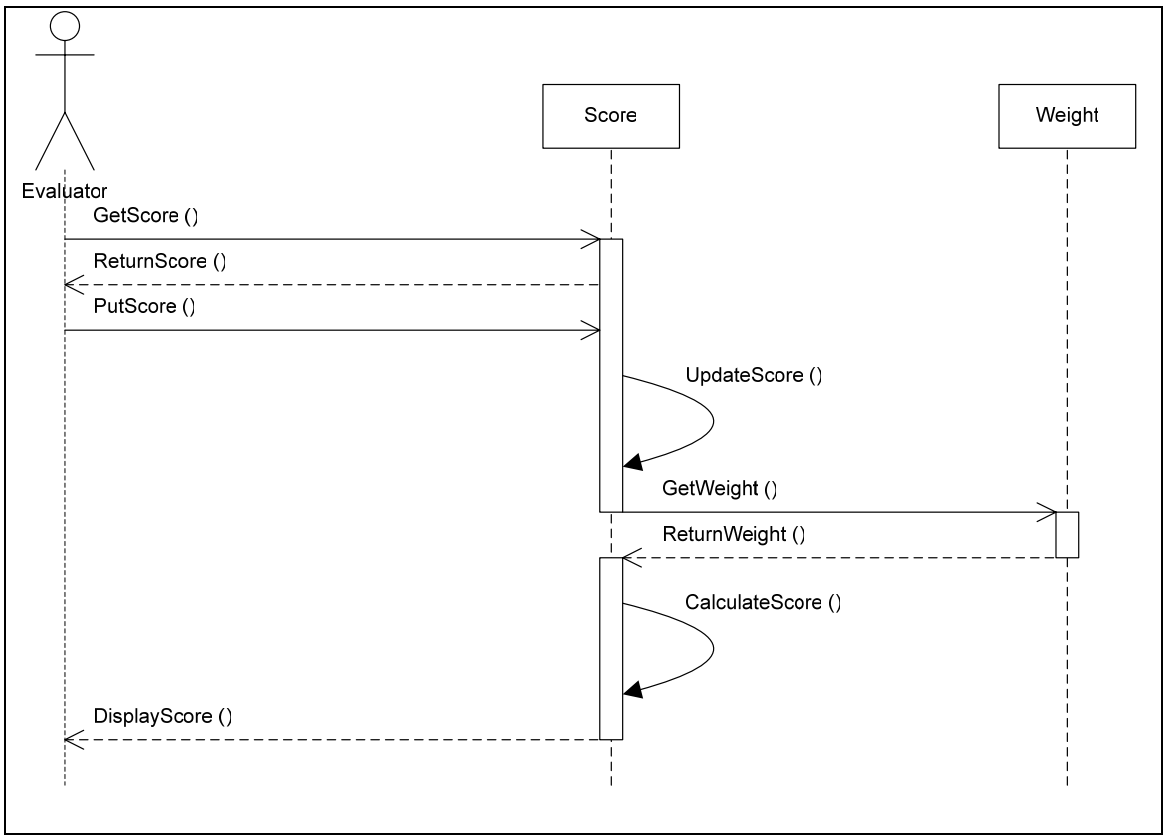

Figure 4.17 Sequence diagram for update score

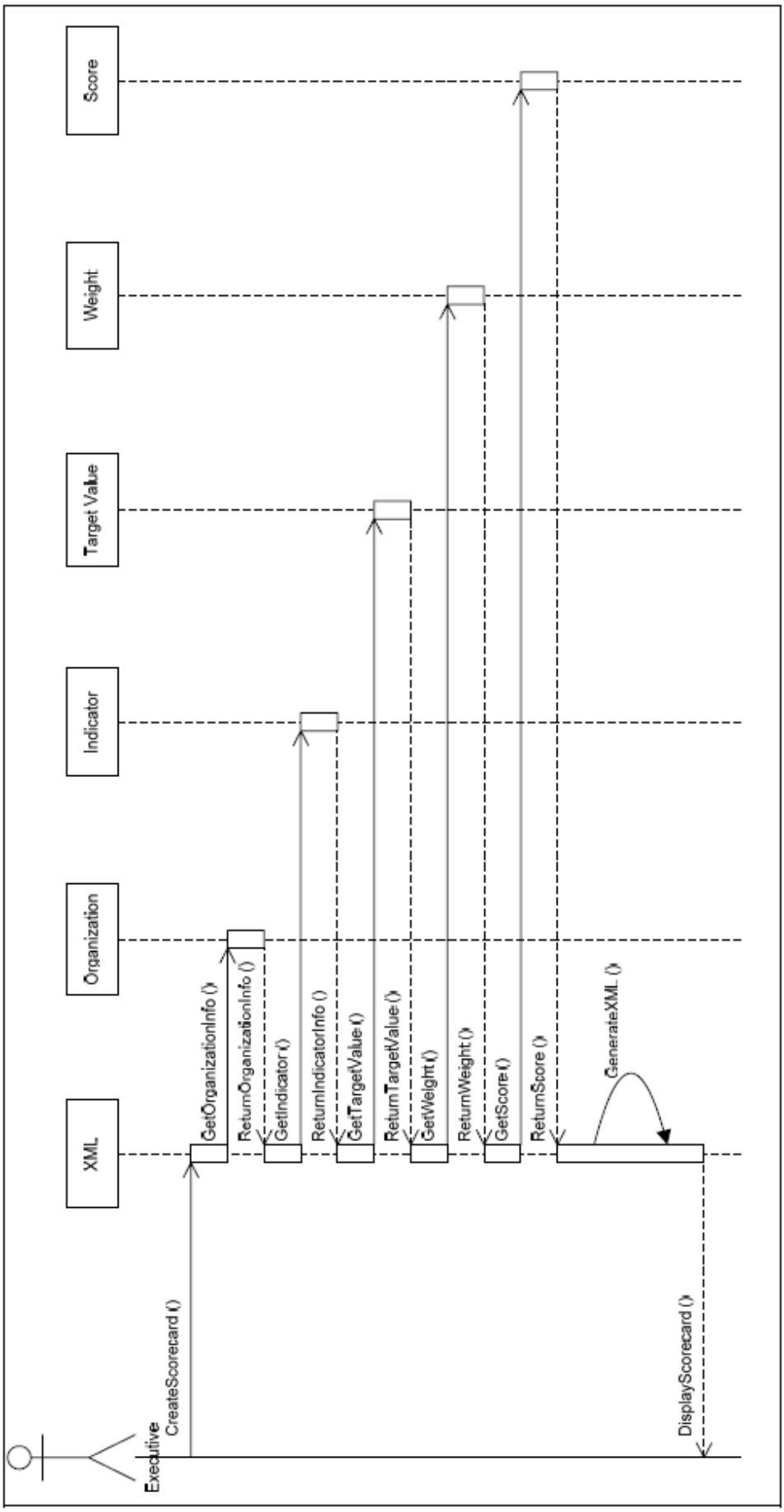

Figure 4.18 Sequence diagram for scorecard

4.4 File structures

In this section, detail of file structure in the prototype system as previously described will be discussed here.

MASTER FILES:

- TOrganization
- TIndicator

TRANSACTION FILES:

- TCountryScore
- TIndScore
- TIndWeight
- TOrgScore
- TProvinceScore
- TPutWeight
- TRegionScore
- TGroupScore

TABLE FILES:

- TDrawWeight
- TExceptionMsg
- TIndicatorType
- TOrganizationType
- TProvince
- TRegion
- TTargetValue
- TUser

4.4.1 List of file structures

MASTER FILES:

Table No.	Name	Description
1	TOrganization	Store all organization
2	TIndicator	Store all indicator

Table 4.1 List of master files.

TRANSACTION FILES:

Table No.	Name	Description
1	TCountryScore	Store organization score
2	TIndScore	Store indicator score group by branch
3	TIndWeight	Store indicator weight group by branch
4	TOrgScore	Store branch score group by branch
5	TProvinceScore	Store province score group by province
6	TPutWeight	Store input weight group by branch
7	TRegionScore	Store region score group by region
8	TGroupScore	Store indicator score group by group

Table 4.2 List of transaction files.

TABLE FILES:

Table No.	Name	Description
1	TDrawWeight	Store indicator for generate metric
2	TExceptionMsg	Store exception message
3	TIndicatorType	Store group of indicator
4	TOrganizationType	Store group of organization
5	TProvince	Store province code and province name
6	TRegion	Store region code and region name
7	TTargetValue	Store target value
8	TUser	Store username and password

Table 4.3 List of table files.

MASTER: TOrganization

Key	Field Name	Data Type	Field Size	Description
PK	sOrgId	nvarchar	4	Organization code
	sOrgName	nvarchar	50	Organization name
	sOrgType	nvarchar	2	Organization type code
	sHomeId	nvarchar	15	Home id
	sStreet	nvarchar	50	Street
	sSubDistrict	nvarchar	50	Sub district
	sDistrict	nvarchar	50	District
	sProvince	nvarchar	2	Province code
	sZipcode	nvarchar	5	Zip code
	sTel	nvarchar	50	Telephone
	sFax	nvarchar	50	Fax
	sUnder	nvarchar	4	Parent of organization
	sUser	nvarchar	20	Create / modify user
	nDate	datetime	8	Create / modify date
	nDelNo	int	4	Flag delete
	nIndex	int	4	Index

Table 4.4 List of torganization fields.

MASTER: TIndicator

Key	Field Name	Data Type	Field Size	Description
PK	sIndId	nvarchar	4	Indicator code
	sIndName	nvarchar	50	Indicator name
	sIndDesc	nvarchar	50	Indicator description
	sIndType	nchar	1	Indicator type code
	sUnder	nvarchar	4	Parent of indicator
	sUser	nvarchar	20	Create / modify user
	nDate	datetime	8	Create / modify date
	nDelNo	int	4	Flag delete
	nIndex	int	4	Index

Table 4.5 List of tindicator fields.

TRANSACTION: TCountryScore

Key	Field Name	Data Type	Field Size	Description
PK	nAssignId	int	4	Assignment code
	nCountryScore	int	4	Score of country
PK	bRC	int	1	Flag is regional center
	sUser	nvarchar	20	Create / modify user
	nDate	int	4	Create / modify date
	nDelNo	int	4	Flag delete
	nIndex	int	4	Index

Table 4.6 List of tcountryscore fields.

TRANSACTION: TIndScore

Key	Field Name	Data Type	Field Size	Description
PK	nAssignId	int	4	Assignment code
PK	sOrgId	nvarchar	4	Organization code
PK	sIndId	nvarchar	4	Indicator code
	nScore	int	4	Score of indicator
	sUser	nvarchar	20	Create / modify user
	nDate	int	4	Create / modify date
	nDelNo	int	4	Flag delete
	nIndex	int	4	Index

Table 4.7 List of tindscore fields.

TRANSACTION: TIndWeight

Key	Field Name	Data Type	Field Size	Description
PK	nAssignId	int	4	Assignment code
PK	sOrgId	nvarchar	4	Organization code
PK	sIndId	nvarchar	4	Indicator code
	nWeight	decimal	9	Weight of indicator
	sUser	nvarchar	20	Create / modify user
	nDate	int	4	Create / modify date
	nDelNo	int	4	Flag delete
	nIndex	int	4	Index

Table 4.8 List of tindweight fields.

TRANSACTION: TOrgScore

Key	Field Name	Data Type	Field Size	Description
PK	nAssignId	int	4	Assignment code
PK	sOrgId	nvarchar	4	Organization code
	nOrgScore	int	4	Score of organization
	sUser	nvarchar	20	Create / modify user
	nDate	int	4	Create / modify date
	nDelNo	int	4	Flag delete
	nIndex	int	4	Index

Table 4.9 List of torgscore fields.

TRANSACTION: TProvinceScore

Key	Field Name	Data Type	Field Size	Description
PK	nAssignId	int	4	Assignment code
PK	sProvinceId	nvarchar	2	Province code
	nProvinceScore	int	4	Score of province
	sUser	nvarchar	20	Create / modify user
	nDate	int	4	Create / modify date
	nDelNo	int	4	Flag delete
	nIndex	int	4	Index

Table 4.10 List of tprovincescore fields.

TRANSACTION: TPutWeight

Key	Field Name	Data Type	Field Size	Description
PK	sOrgId	nvarchar	4	Organization code
PK	sUnder	nvarchar	4	Parent of indicator
PK	nX	int	4	Position x
PK	nY	int	4	Position y
	nWeight	decimal	9	Weight of position
	sUser	nvarchar	20	Create / modify user
	nDate	int	4	Create / modify date
	nDelNo	int	4	Flag delete
	nIndex	int	4	Index

Table 4.11 List of tputweight fields.

TRANSACTION: TRegionScore

Key	Field Name	Data Type	Field Size	Description
PK	nAssignId	int	4	Assignment code
PK	sRegionId	nvarchar	2	Region code
	nRegScore	int	4	Score of region
PK	bRC	int	1	Flag is regional center
	sUser	nvarchar	20	Create / modify user
	nDate	int	4	Create / modify date
	nDelNo	int	4	Flag delete
	nIndex	int	4	Index

Table 4.12 List of tregionscore fields.

TRANSACTION: TGroupScore

Key	Field Name	Data Type	Field Size	Description
PK	nAssignId	int	4	Assignment code
PK	sGroupId	nvarchar	2	Group code
PK	sGroupType	nchar	1	Group Type (P : Province, R : Region, A : All)
PK	sIndId	nvarchar	4	Indicator code
	nIndScore	int	4	Indicator score
	sUser	nvarchar	20	Create / modify user
	nDate	int	4	Create / modify date
	nDelNo	int	4	Flag delete
	nIndex	int	4	Index

Table 4.13 List of tgroupscore fields.

TABLE: TDrawWeight

Key	Field Name	Data Type	Field Size	Description
PK	sIndType	nchar	1	Indicator type code
PK	sUnder	nvarchar	4	Parent of indicator
PK	nItemId	int	4	Code of draw indicator
	sIndId	nvarchar	4	Indicator code
	sUser	nvarchar	20	Create / modify user
	nDate	datetime	8	Create / modify date
	nDelNo	int	4	Flag delete
	nIndex	int	4	Index

Table 4.14 List of tdrawweight fields.

TABLE: TExceptionMsg

Key	Field Name	Data Type	Field Size	Description
PK	sMsgId	nvarchar	6	Message code
	sMsgDesc	nvarchar	100	Message description
	sUser	nvarchar	20	Create / modify user
	nDate	datetime	8	Create / modify date
	nDelNo	int	4	Flag delete
	nIndex	int	4	Index

Table 4.15 List of texceptionmsg fields.

TABLE: TIndicatorType

Key	Field Name	Data Type	Field Size	Description
PK	sIndType	nchar	1	Indicator type code
	sIndTypeDesc	nvarchar	50	Indicator type description
	sUser	nvarchar	20	Create / modify user
	nDate	datetime	8	Create / modify date
	nDelNo	int	4	Flag delete
	nIndex	int	4	Index

Table 4.16 List of tindicatortype fields.

TABLE: TOrganizationType

Key	Field Name	Data Type	Field Size	Description
PK	sOrgTypeId	nvarchar	2	Organization type code
	sOrgTypeName	nvarchar	50	Organization type description
	sUser	nvarchar	20	Create / modify user
	nDate	datetime	8	Create / modify date
	nDelNo	int	4	Flag delete
	nIndex	int	4	Index

Table 4.17 List of torganizationtype fields.

TABLE: TProvince

Key	Field Name	Data Type	Field Size	Description
PK	sProvinceId	nvarchar	2	Province code
	sProvinceName	nvarchar	50	Province name
	sRegionId	nvarchar	2	Region code
	sUser	nvarchar	20	Create / modify user
	nDate	datetime	8	Create / modify date
	nDelNo	int	4	Flag delete
	nIndex	int	4	Index

Table 4.18 List of tprovince fields.

TABLE: TRegion

Key	Field Name	Data Type	Field Size	Description
PK	sRegionId	nvarchar	2	Region code
	sRegionName	nvarchar	50	Region name
	sUser	nvarchar	20	Create / modify user
	nDate	datetime	8	Create / modify date
	nDelNo	int	4	Flag delete
	nIndex	int	4	Index

Table 4.19 List of tregion fields.

TABLE: TTargetValue

Key	Field Name	Data Type	Field Size	Description
PK	sTargetId	nvarchar	2	Target value code
	nRedFrom	int	4	Start red color
	nRedTo	int	4	End red color
	nYellowFrom	int	4	Start yellow color
	nYellowTo	int	4	End yellow color
	nGreenFrom	int	4	Start green color
	nGreenTo	int	4	End green color
	sUser	nvarchar	20	Create / modify user
	nDate	datetime	8	Create / modify date
	nDelNo	int	4	Flag delete
	nIndex	int	4	Index

Table 4.20 List of ttargetvalue fields.

TABLE: TUser

Key	Field Name	Data Type	Field Size	Description
PK	sUserId	nvarchar	4	User code
	sUserName	nvarchar	10	User name
	sPassword	nvarchar	10	Password
	sOrgId	nvarchar	4	Organization code
	sFName	nvarchar	50	First name
	sLName	nchar	50	Last name
	sUser	nvarchar	20	Create / modify user
	nDate	datetime	8	Create / modify date
	nDelNo	int	4	Flag delete
	nIndex	int	4	Index

Table 4.21 List of tuser fields.

4.5 Module specification

Module Name	**Create Branch**
Description	This process perform create branch (Regional Center, Branch).
Input	Organization Name [required] Organization Alias [required] Organization Type [required] Home id [optional] Street [optional] Sub district [optional] District [optional] Province [required] Zip code [optional] Telephone [optional] Fax [optional] Parent Organization [optional]
Output	Branch record has been created
Logical Summary	
	Insert record in TOrganization table IF Regional Center THEN SET sOrgType = '02' AND sUnder = '0' ELSE sOrgType = '03' AND sUnder = 'Reginal Center Id' Assign sOrgId, sOrgName, sOrgType, sHomeId, sStreet, sSubDistrict, sDistrict, sProvince, sZipcode, sTel, sFax, sUnder, nDate, nDelNo

Module Name	**Update Branch**
Description	This process perform update branch (Regional Center, Branch).
Input	Organization Name [required] Organization Alias [required] Organization Type [required] Home id [optional] Street [optional] Sub district [optional] District [optional] Province [required] Zip code [optional] Telephone [optional] Fax [optional] Parent Organization [optional]
Output	Branch record has been updated.
Logical Summary	
	Update record in TOrganization table Update fields: sOrgId, sOrgName, sOrgType, sHomeId, sStreet, sSubDistrict, sDistrict, sProvince, sZipcode, sTel, sFax, sUnder, nDate

Module Name	**View Branch**
Description	This process show branch information (Regional Center, Branch).
Input	Organization Id
Output	Branch Information.
Logical Summary	
1. Select record in Torganization Table. 2. Display selected organization record and display following information: sOrgName, sOrgType, sHomeId, sStreet, sSubDistrict, sDistrict, sProvince, sZipcode, sTel, sFax, sUnder	

Module Name	**Create Indicator**
Description	This process perform create component (Perspective, Objective, Measure).
Input	Indicator Name [required] Indicator Alias [required] Indicator Type [required] Indicator Description [optional] Parent Indicator [optional]
Output	Indicator record has been created.
Logical Summary	
	Insert record in TIndicator table IF Indicator As Perspective THEN sIndType = 'P' AND sUnder = '0' ELSE IF Indicator As Objective THEN sIndType = 'O' AND sUnder = 'Perspective Id' ELSE sIndType = 'M' AND sUnder = 'Objective Id' Assign sIndId, sIndName, sIndType, sIndDesc, sUnder, sUser, nDate, nDelNo

Module Name	**Update Indicator**
Description	This process perform update component (Perspective, Objective, Measure).
Input	Indicator Name [required] Indicator Alias [required] Indicator Type [required] Indicator Description [optional] Parent Indicator [optional]
Output	Indicator record has been updated.
Logical Summary	
	Update record in TIndicator table Update fields: sIndId, sIndName, sIndType, sIndDesc, sUnder, sUser, nDate, nDelNo

Module Name	**View Indicator**
Description	This process display indicator information(Perspective, Objective, Measure).
Input	Indicator Id
Output	Indicator Information.
Logical Summary	
	1. Select record in TIndicator table. 2. Display selected indicator record and display following information: sIndName, sIndType, sIndDesc, sUnder

Module Name	**Update Target Value**
Description	This process perform update target values.
Input	Range of red color [required] Range of yellow color [required] Range of green color [required]
Output	Target values record has been updated.
Logical Summary	
	Update record in TTargetValue table Update Condition: nRedFrom = 0 nGreenFrom = 100 nRedFrom < nRedTo nRedTo < nYellowwFrom nYellowFrom < nYellowTo nYellowTo < nGreenTo nGreenTo < nGreenFrom Update fields: nRedFrom, nRedTo, nYellowFrom, nYellowTo, nGreenTo, nGreenFrom, sUser, nDate

Module Name	**Initialize Weight**
Description	This process perform initial weight.
Input	Organization Id [required] Priority of indicator [required]
Output	All measurement records has been created.
Logical Summary	
1.	Verify existing assignment IF Organization have existing assignment THEN EXIT this step ELSE Insert all indicator Id to TIndScore by set nScore = 0
2.	Insert priority value of perspectives to TPutWeight.
3.	Calculate weight with AHP method
4.	Insert weight of each perspective to TIndWeight
5.	Display weight value of each perspective
6.	Insert priority value of objectives to TPutWeight.
7.	Calculate weight with AHP method
8.	Insert weight of each objective to TIndWeight
9.	Display weight value of each objective
10.	Insert priority value of measures to TPutWeight.
11.	Calculate weight with AHP method
12.	Insert weight of each measure to TIndWeight
13.	Display weight value of each measure

Module Name	**Initialize Score**
Description	This process perform initial score.
Input	Indicator Id [required] Organization Id [required] Weight of indicator [required] Score of indicator [required]
Output	Score records has been created.
Logical Summary	
1.	Insert all scores of measure to TIndScore
2.	Calculate scores of objective and perspective $S(Parent) = \sum_{i=1}^{n} \frac{(S(Child_i) \times W(Child_i))}{100}$
3.	Update scores of objective and perspective to TIndScore
4.	Calculate score of branch $S(Parent) = \sum_{i=1}^{n} \frac{(S(Child_i) \times W(Child_i))}{100}$
5.	Update score of branch to TOrgScore
6.	Calculate score of province, score of region and score of organization $S(Parent) = Avg(S(Child_1), S(Child_2), ..., S(Child_n))$
7.	update score to TProvinceScore, TRegionScore and TCountryScore
8.	Display scores of measure

Module Name	**Update Weight**
Description	This process perform update weight of each indicators (Perspective, Objective, Measure).
Input	Indicator Id [required] Organization Id [required] Priority of indicator [required]
Output	Weight of specify indicators record has been updated.
Logical Summary	
1.	Update priority value of indicators to TPutWeight.
2.	Recalculate weight with AHP method
3.	Update weight of indicator to TIndWeight
4.	Recalculate scores of objective and perspective $S(Parent) = \sum_{i=1}^{n} \frac{(S(Child_i) \times W(Child_i))}{100}$
5.	Update scores of objective and perspective to TIndScore
6.	Recalculate score of branch $S(Parent) = \sum_{i=1}^{n} \frac{(S(Child_i) \times W(Child_i))}{100}$
7.	Update score of branch to TOrgScore
8.	Recalculate score of province, score of region and score of organization $S(Parent) = Avg(S(Child_1), S(Child_2), ..., S(Child_n))$
9.	Update score to TProvinceScore, TRegionScore and TCountryScore
10.	Display weight

Module Name	**View Weight**
Description	This process shows indicator weight information.
Input	Indicator Id[required] Organization Id[required]
Output	Indicator Weight information.
Logical Summary	
1.	Select record in Tindicator, TIndWeight tables.
2.	Display selected Tindicator and TIndWeight record.

Module Name	**Update Score**
Description	This process perform update indicator score action and will apply only Measure type
Input	Indicator Id [required] Organization Id [required] Indicator Score [required]
Output	Score of specify indicators has been updated.
Logical Summary	
1.	Update score of measure in TIndScore.
2.	Recalculate scores of objective and perspective $S(Parent) = \sum_{i=1}^{n} \frac{(S(Child_i) \times W(Child_i))}{100}$
3.	Update scores of objective and perspective to TIndScore
4.	Recalculate score of branch $S(Parent) = \sum_{i=1}^{n} \frac{(S(Child_i) \times W(Child_i))}{100}$
5.	Update score of branch to TOrgScore
6.	Recalculate score of province, score of region and score of organization

	$S(Parent) = Avg(S(Child_1), S(Child_2), ..., S(Child_n))$
7.	Update score to TProvinceScore, TRegionScore and TCountryScore
8.	Display scores of measure

Module Name	**View Score**
Description	This process shows indicator score.
Input	Indicator Id[required] Organization Id[required]
Output	Indicator score information.
Logical Summary	
1.	Select record in Tindicator, TIndScore tables.
2.	Display selected Tindicator and TIndScore record.

Module Name	**Calculate Summary Score**
Description	This process perform calculate score of perspective, objective and measure group by province, region and organization.
Input	Indicator Id [required] Organization Id [required] Score of indicator [required]
Output	Score of perspective, objective and measure has been created group by province, region and organization.
Logical Summary	
1.	Select scores of indicator from TIndScore
2.	Calculate scores of measure $S(M_{Parent}) = Avg(S(M_{Child_1}), S(M_{Child_2}), ..., S(M_{Child_n}))$
3.	Update scores of measure to TGroupScore
4.	Calculate scores of objective and perspective $S(Parent) = Avg(S(Child_1), S(Child_2), ..., S(Child_n))$
5.	Update scores of objective and perspective to TGroupScore

Module Name	**Generate XML file**
Description	This process generate scorecard.
Input	nAssignId [required]
Output	Xml file has been generated.
Logical Summary	
	Construct xml file: IF BAAC-Regional Centers THEN IF 'Table' Type THEN Generate Xml File following 'Table_scorecard' structure ELSE Generate Xml File following 'Tree_scorecard' structure END END ELSE IF BAAC-Branches THEN IF 'Table' Type THEN Generate Xml File following 'Table_scorecard' structure ELSE Generate Xml File following 'Tree_scorecard' structure END END ELSE IF Region-Regional Centers THEN IF 'Table' Type THEN Generate Xml File following 'Table_scorecard' structure ELSE

	Generate Xml File following 'Tree_scorecard' structure END END ELSE IF Regions-Branches THEN IF 'Table' Type THEN Generate Xml File following 'Table_scorecard' structure ELSE Generate Xml File following 'Tree_scorecard' structure END END ELSE IF Province THEN IF 'Table' Type THEN Generate Xml File following 'Table_scorecard' structure ELSE Generate Xml File following 'Tree_scorecard' structure END END ELSE IF ORGANIZATION THEN IF 'Table' Type THEN Generate Xml File following 'Table_scorecard' structure ELSE Generate Xml File following 'Tree_scorecard' structure END END ELSE IF PERSPECTIVE

	THEN IF 'Table' Type THEN Generate Xml File following 'Table_scorecard' structure ELSE Generate Xml File following 'Perspective' structure END END

Module Name	**Display Scorecard**
Description	This process show scorecard report
Input	XML File
Output	Scorecard Report
Logical Summary	

	IF File_Name = 'Table_scorecard' THEN
	Select data from XML file and display scorecard in a table form
	ELSE IF File_Name = 'Tree_scorecard' THEN
	Select data from XML file and display scorecard in a tree form
	ELSE
	Select data from XML file and display scorecard in a tree form
	END

CHAPTER V
SYSTEM IMPLEMENTATION

This chapter describes system environment, system tools and resources, program structure and XML structure.

5.1 System environment

The computer used for development of the system is Intel Centrino Pentium M 1.3 GHz, RAM 256 Mbytes, running under Microsoft Window XP SP1.

5.2 System tools and resources

The development programming language is jsp. The software used in this research project is as follows:

- Apache Tomcat Server 4.1
- Macromedia Dreamweaver 8
- Macromedia Flash 8
- Macromedia Flash Player 8
- Microsoft SQL Server 2000
- Java(TM) 2 SDK, Standard Edition 1.4.2_03
- Edit Plus Text Editor v2.01b

5.3 Program structure

This section reveals the program structure of source codes.

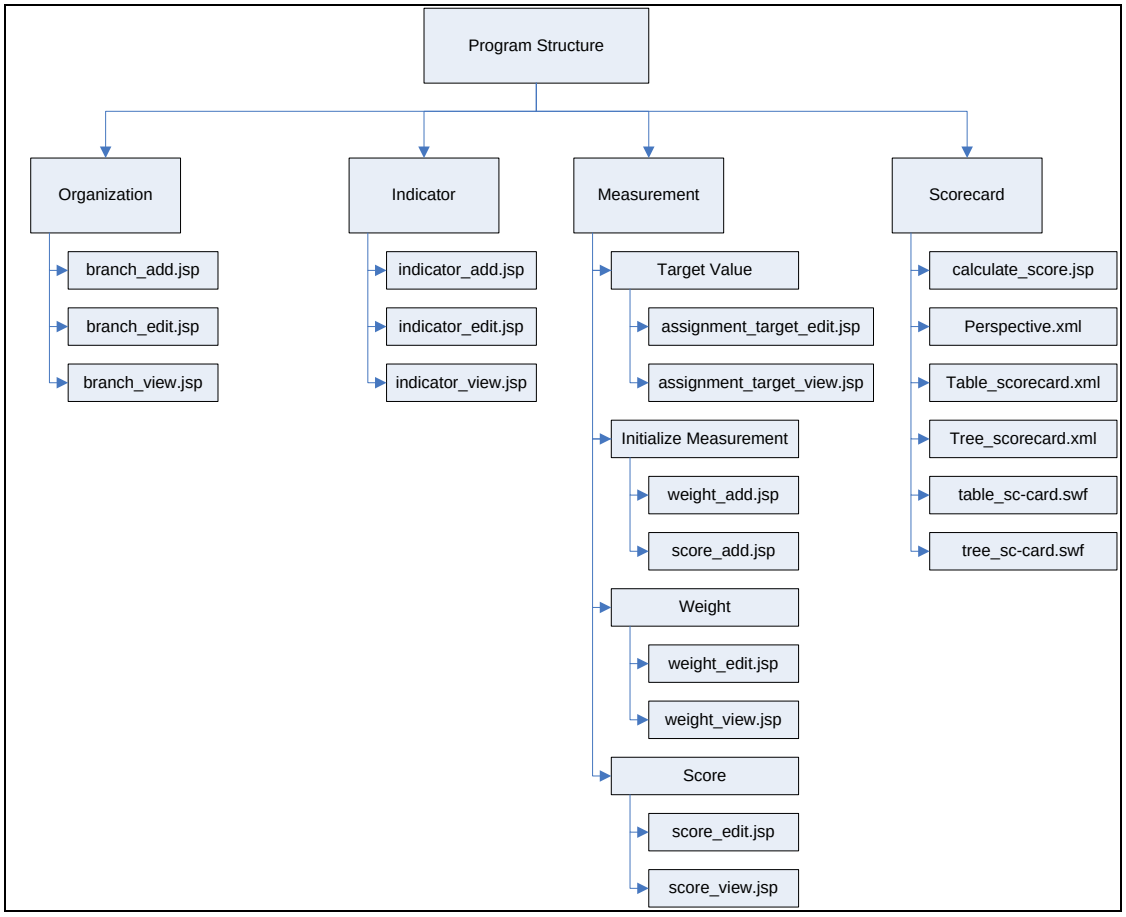

Figure 5.1 Program structure

5.4 XML structure

This section reveals XML structure of perspective, Table_Scorecard and Tree_Scorecard file.

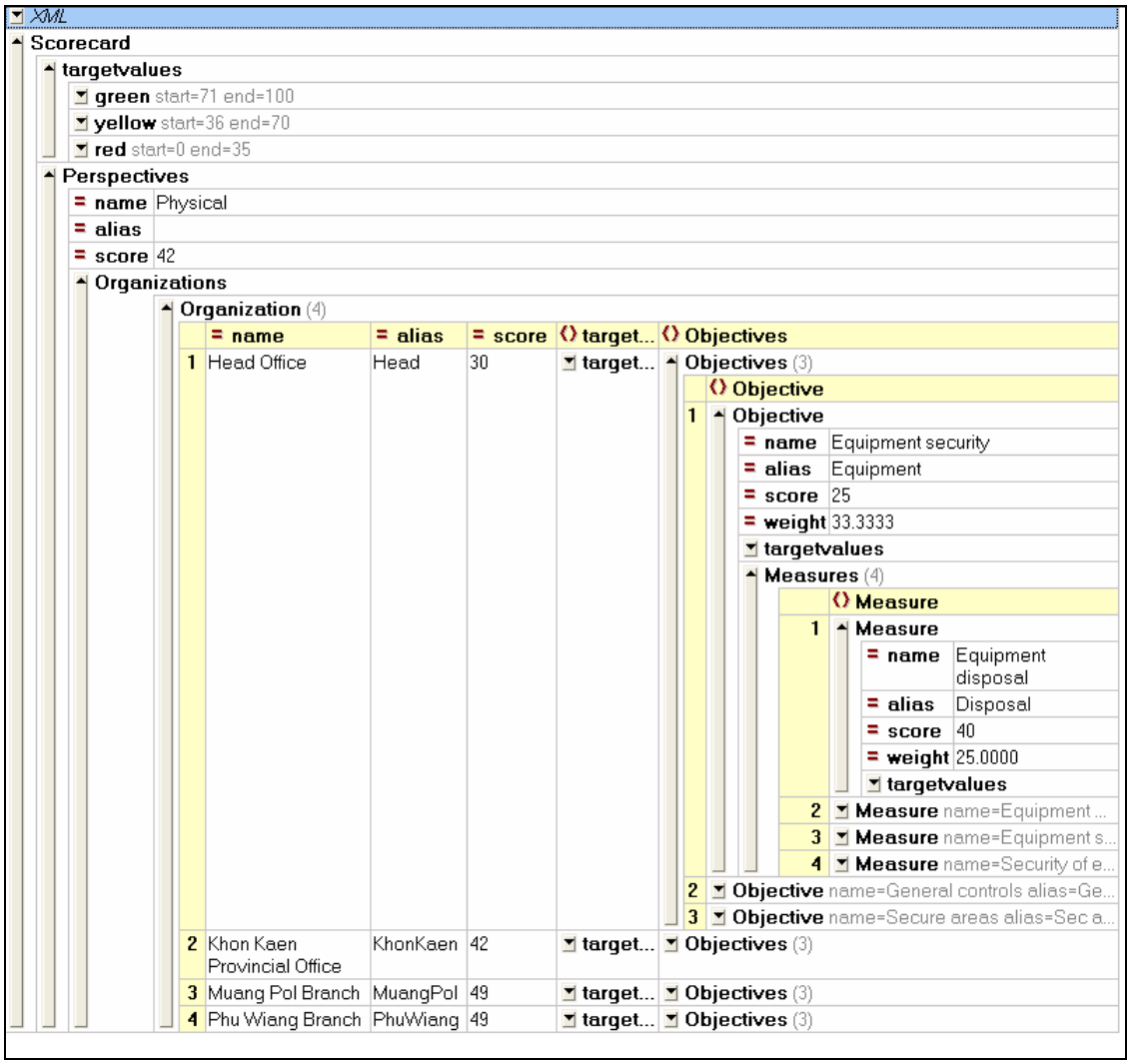

Figure 5.2 Perspective XML structure

Figure 5.2 shows XML structure of perspective file which represents the evaluation results of the perspective in tree form.

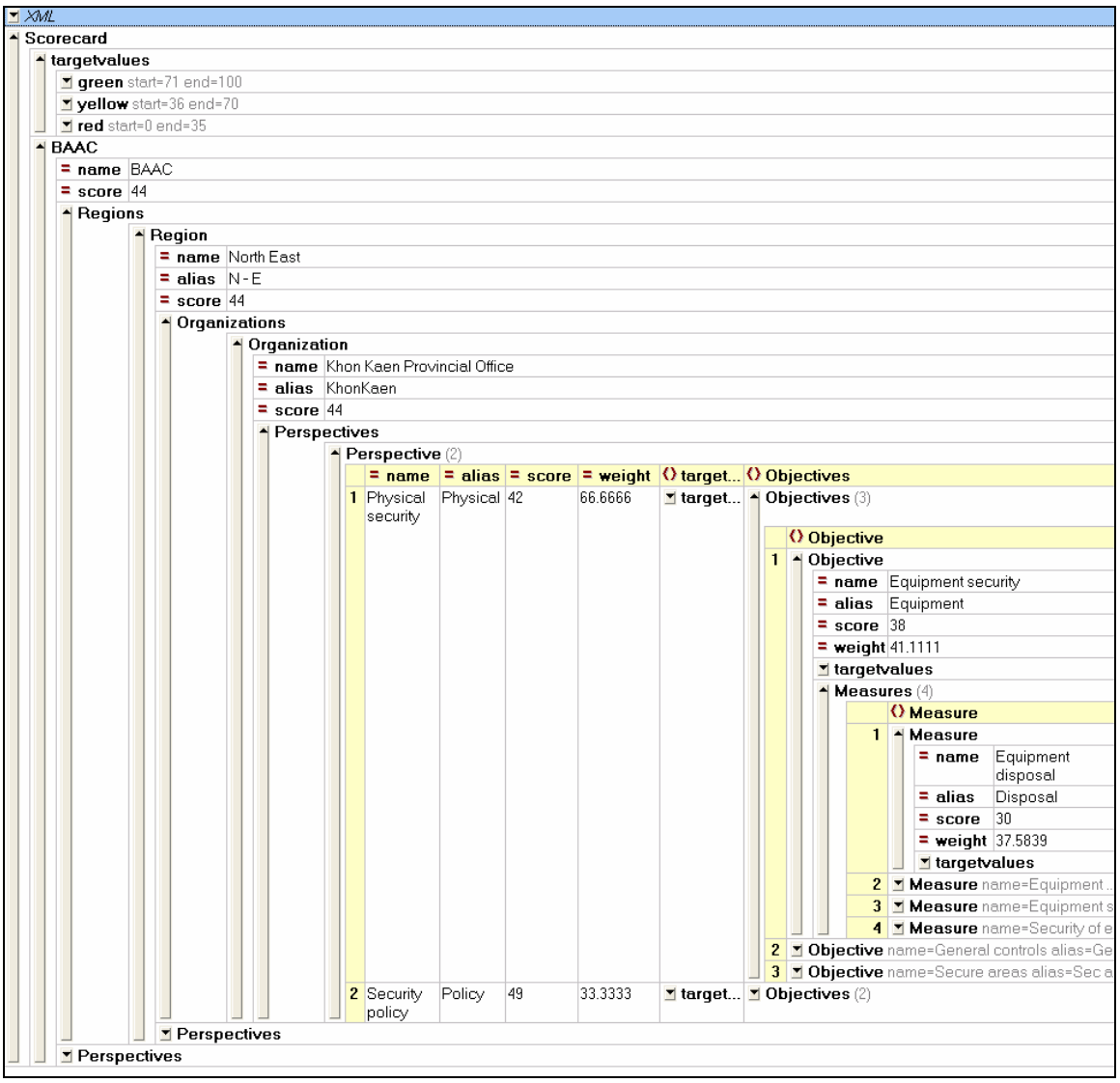

Figure 5.3 Table_Scorecard XML structure

Figure 5.3 shows XML structure of Table_Scorecard file which represents the evaluation results in table form.

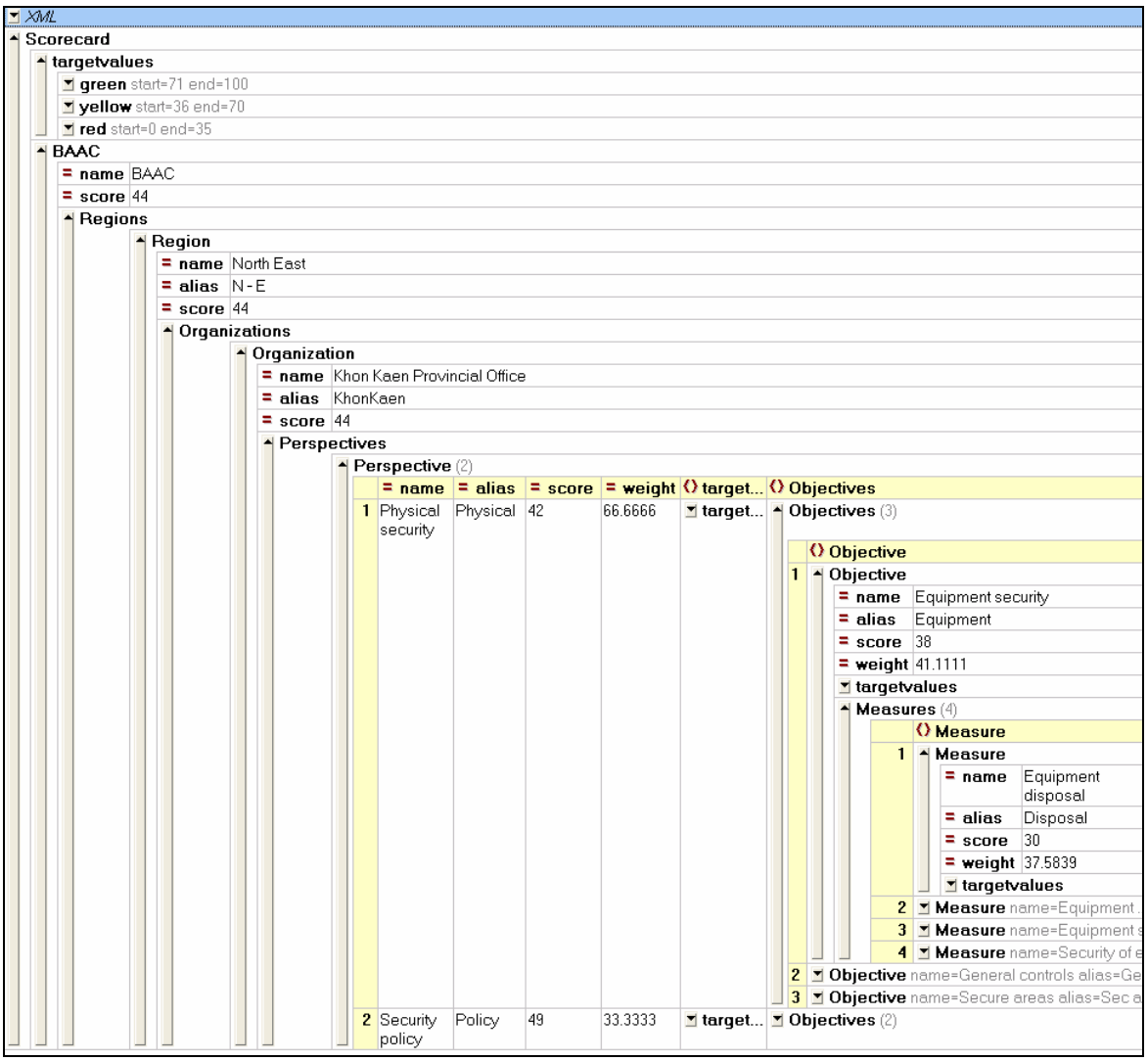

Figure 5.4 Tree_Scorecard XML structure

Figure 5.4 shows XML structure of Tree_Scorecard file which represents the evaluation results in tree form.

CHAPTER VI
EXPERIMENTAL RESULTS

This chapter demonstrates the experimental results of the developed ICT security evaluation system. The system consists of 2 major indicators, namely, measurement and scorecard. Measurement is the definition of evaluation value while scorecard is the tool to display evaluation results represented in tree and table formats.

6.1 Measurement

Measurement is the specification of ICT security assessment concerning with the definition of target value, weight and score.

6.1.1 Target value assignment

There are 3 color ranges of target value assignment, red, yellow and green which represent 3 levels of assessment result, poor, fair and good respectively. Each level also has ranges of score as shown in figures 6.1.

Red - poor.

Yellow - fair.

Green - good.

Target Value			
Indicator	Range		
	0	**to**	30
	31	**to**	70
	71	**to**	**100**

Figure 6.1 Target Value

Figure 6.1 illustrates the score ranges and assessment results, score 0-30 means “Poor” colored with red, 31-70 indicates “Fair” colored with yellow and 71-100 implies “Good” colored with green.

6.1.2 Weight assignment

To evaluate ICT security, we need to define weight values for each branch. Weight values are derived from component prioritization via Analytic Hierarchy Process (AHP). Finally, weight values will be calculated with score to get the assessment results. The changes in weight value would affect to the assessment results.

6.1.2.1 Initial weight

Initial weight is the weight definition of the first evaluation for each branch which all components of the system will be assessed with the same weight assignment method in the following order, perspective, objective and measure.

	Contingency Planning and Disaster Recovery	Data Security	Facility security	Hardware security	Incident Reporting	Network Security	Personnel security	Physical security	Regulatory Security	Security policy	Software security
Contingency Planning and Disaster Recovery	1										
Data Security		1									
Facility security			1								
Hardware security				1							
Incident Reporting					1						
Network Security						1					
Personnel security							1				
Physical security								1			
Regulatory Security									1		
Security policy										1	
Software security											1

Figure 6.2 Displays the screen of perspective prioritization

Figure 6.2 views the screen of perspective prioritization in which program will prioritize 11 perspectives by comparing and scoring each perspective in accordance with the prioritization table. The estimator will only input value in the above rectangle then program will automatically calculate for the rest. Both objective and measure prioritization will apply with the same method as perspective prioritization by which estimator will conduct component comparison and prioritization for each parent.

Weight Information of **x**		Weight Information of **y (Inverse of x)**	
1	Measure **x** and **y** are of equal importance	**1**	Measure **y** and **x** are of equal importance
3	Measure **x** is weakly more importance than **y**	**0.33**	Measure **y** is weakly more importance than **x**
5	Measure **x** is strongly more importance than **y**	**0.2**	Measure **y** is strongly more importance than **x**
7	Measure **x** is very strongly more importance than **y**	**0.14**	Measure **y** is very strongly more importance than **x**
9	Measure **x** is absolutely more important than **y**	**0.11**	Measure **y** is absolutely more important than **x**
2,4,6,8	Intermediate values	**0.5,0.25,0.16,0.12**	Intermediate values

Table 6.1 Prioritization table

	Contingency Planning and Disaster Recovery	Data Security	Facility security	Hardware security	Incident Reporting	Network Security	Personnel security	Physical security	Regulatory Security	Security policy	Software security
Contingency Planning and Disaster Recovery	1	3	0.5	2.0	0.33	0.2	0.2	0.33	2	0.11	2
Data Security		1	0.33	2	3	0.33	2	3	3	0.5	2
Facility security			1	3	4	2	0.33	0.5	0.5	3	3
Hardware security				1	4	0.5	2	2	2	0.5	4
Incident Reporting					1	0.5	0.33	0.5	0.5	0.2	2
Network Security						1	2	3	2	0.5	2
Personnel security							1	0.5	0.33	0.2	1
Physical security								1	3	0.33	2
Regulatory Security									1	5	2
Security policy										1	3
Software security											1

Figure 6.3 Example Inputs of Perspective Prioritization

Figure 6.3 depicts example inputs of Perspective Prioritization such that the comparison between data and facility security has priority value of 0.33 which means facility security is more important than data security for 3 times.

	Contingency Planning and Disaster Recovery	Data Security	Facility security	Hardware security	Incident Reporting	Network Security	Personnel security	Physical security	Regulatory Security	Security policy	Software security	Average	Weigh
Contingency Planning and Disaster Recovery	0.0333	0.2061	0.0471	0.1428	0.0122	0.0239	0.0105	0.0224	0.133	0.0094	0.0833	0.0658	6.5877
Data Security	0.0111	0.0687	0.0311	0.1428	0.1116	0.0394	0.1058	0.2042	0.1996	0.0428	0.0833	0.0948	9.4625
Facility security	0.0667	0.2082	0.0943	0.2142	0.1489	0.2392	0.0174	0.034	0.0332	0.257	0.125	0.1307	13.0781
Hardware security	0.0166	0.0343	0.0314	0.0714	0.1489	0.0598	0.1058	0.1361	0.133	0.0428	0.1666	0.0861	8.6113
Incident Reporting	0.101	0.0229	0.0235	0.0178	0.0372	0.0598	0.0174	0.034	0.0332	0.0171	0.0833	0.0407	4.0701
Network Security	0.1667	0.2082	0.0471	0.1428	0.0744	0.1196	0.1058	0.2042	0.133	0.0428	0.0833	0.1207	12.0772
Personnel security	0.1667	0.0343	0.2858	0.0357	0.1128	0.0598	0.0529	0.034	0.0219	0.0171	0.0416	0.0784	7.8463
Physical security	0.101	0.0229	0.1886	0.0357	0.0744	0.0398	0.1058	0.068	0.1996	0.0282	0.0833	0.0861	8.617
Regulatory Security	0.0166	0.0229	0.1886	0.0357	0.0744	0.0598	0.1604	0.0226	0.0665	0.4284	0.0833	0.1054	10.5425
Security policy	0.3032	0.1374	0.0314	0.1428	0.1861	0.2392	0.2646	0.2062	0.0133	0.0856	0.125	0.1577	15.7758
Software security	0.0166	0.0343	0.0314	0.0178	0.0186	0.0598	0.0529	0.034	0.0332	0.0285	0.0416	0.0335	3.3567

Figure 6.4 Results from Weight Calculation of Perspective

In figure 6.4, after perspective prioritization, our program will calculate weight for each perspective by using AHP technique. The weight summation of component within the same parent is equal to 100.

6.1.2.2 Weight after adjustment

The changes in weight will change component priority. The weight adjustment can be applied in 3 parts that is weight of perspective, objective and measure.

- Perspective's weight – adjusting weight of perspective, the program will re-calculate perspective, branch, province, region and organization score which will affect to the assessment results.
- Objective's weight – changing weight of objective, the program will re-calculate perspective, branch, province, region and organization score which will affect to the assessment results.
- Measure's weight – editing weight of measure, the program will re-calculate perspective, branch, province, region and organization score which will affect to the assessment results.

	Contingency Planning and Disaster Recovery	Data Security	Facility security	Hardware security	Incident Reporting	Network Security	Personnel security	Physical security	Regulatory Security	Security policy	Software security
Contingency Planning and Disaster Recovery	1	3.0	0.5	2.0	0.33	0.2	0.2	0.33	2.0	0.11	2.0
Data Security		1	0.33	2.0	3.0	0.33	2.0	3.0	3.0	0.5	2.0
Facility security			1	3.0	4.0	2.0	0.33	0.5	0.5	3.0	3.0
Hardware security				1	4.0	0.5	2.0	2.0	2.0	0.5	4.0
Incident Reporting					1	0.5	0.33	0.5	0.5	0.2	2.0
Network Security						1	2.0	3.0	2.0	0.5	2.0
Personnel security							1	0.5	0.33	0.2	1.0
Physical security								1	3.0	0.33	2.0
Regulatory Security									1	5.0	2.0
Security policy										1	3.0
Software security											1

Figure 6.5 Weight values of each perspective before edition.

	Contingency Planning and Disaster Recovery	Data Security	Facility security	Hardware security	Incident Reporting	Network Security	Personnel security	Physical security	Regulatory Security	Security policy	Software security
Contingency Planning and Disaster Recovery	1	0.33	0.5	0.2	0.33	0.2	0.2	0.33	2.0	0.11	0.11
Data Security		1	0.33	2.0	3.0	0.33	2.0	3.0	3.0	0.5	2.0
Facility security			1	3.0	4.0	2.0	0.33	0.5	0.5	3.0	3.0
Hardware security				1	4.0	0.5	2.0	2.0	2.0	0.5	4.0
Incident Reporting					1	0.5	0.33	0.5	0.5	0.2	2.0
Network Security						1	2.0	3.0	2.0	0.5	2.0
Personnel security							1	0.5	0.33	0.2	1.0
Physical security								1	3.0	0.33	2.0
Regulatory Security									1	5.0	2.0
Security policy										1	3.0
Software security											1

Figure 6.6 Weight values of each perspective after edition.

Figure 6.5 and 6.6 present perspective prioritization before and after edition. This example shows edition of contingency planning and other perspectives.

	Contingency Planning and Disaster Recovery	Data Security	Facility security	Hardware security	Incident Reporting	Network Security	Personnel security	Physical security	Regulatory Security	Security policy	Software security	Average	Weight
Contingency Planning and Disaster Recovery	0.0333	0.2061	0.0471	0.1428	0.0122	0.0239	0.0105	0.0224	0.133	0.0094	0.0833	0.0658	6.5877
Data Security	0.0111	0.0687	0.0311	0.1428	0.1116	0.0394	0.1058	0.2042	0.1996	0.0428	0.0833	0.0946	9.4625
Facility security	0.0667	0.2082	0.0943	0.2142	0.1489	0.2392	0.0174	0.034	0.0332	0.257	0.125	0.1307	13.0781
Hardware security	0.0166	0.0343	0.0314	0.0714	0.1489	0.0598	0.1058	0.1361	0.133	0.0428	0.1666	0.0861	8.6113
Incident Reporting	0.101	0.0229	0.0235	0.0178	0.0372	0.0598	0.0174	0.034	0.0332	0.0171	0.0833	0.0407	4.0701
Network Security	0.1667	0.2082	0.0471	0.1428	0.0744	0.1196	0.1058	0.2042	0.133	0.0428	0.0833	0.1207	12.0772
Personnel security	0.1667	0.0343	0.2858	0.0357	0.1128	0.0598	0.0529	0.034	0.0219	0.0171	0.0416	0.0784	7.8463
Physical security	0.101	0.0229	0.1886	0.0357	0.0744	0.0398	0.1058	0.068	0.1996	0.0282	0.0833	0.0861	8.617
Regulatory Security	0.0166	0.0229	0.1886	0.0357	0.0744	0.0598	0.1604	0.0226	0.0665	0.4284	0.0833	0.1054	10.5425
Security policy	0.3032	0.1374	0.0314	0.1428	0.1861	0.2392	0.2646	0.2062	0.0133	0.0856	0.125	0.1577	15.7758
Software security	0.0166	0.0343	0.0314	0.0178	0.0186	0.0598	0.0529	0.034	0.0332	0.0285	0.0416	0.0335	3.3567

Figure 6.7 All weight values of each perspective before edition.

	Contingency Planning and Disaster Recovery	Data Security	Facility security	Hardware security	Incident Reporting	Network Security	Personnel security	Physical security	Regulatory Security	Security policy	Software security	Average	Weight
Contingency Planning and Disaster Recovery	0.0218	0.0277	0.0471	0.0163	0.0122	0.0239	0.0105	0.0224	0.133	0.0094	0.0049	0.0299	2.9992
Data Security	0.0662	0.0841	0.0311	0.1639	0.1116	0.0394	0.1058	0.2042	0.1996	0.0428	0.0904	0.1036	10.3601
Facility security	0.0436	0.255	0.0943	0.2459	0.1489	0.2392	0.0174	0.034	0.0332	0.257	0.1356	0.1367	13.679
Hardware security	0.1092	0.042	0.0314	0.0819	0.1489	0.0598	0.1058	0.1361	0.133	0.0428	0.1809	0.0974	9.7483
Incident Reporting	0.0662	0.028	0.0235	0.0204	0.0372	0.0598	0.0174	0.034	0.0332	0.0171	0.0904	0.0388	3.8886
Network Security	0.1092	0.255	0.0471	0.1639	0.0744	0.1196	0.1058	0.2042	0.133	0.0428	0.0904	0.1223	12.236
Personnel security	0.1092	0.042	0.2858	0.0409	0.1128	0.0598	0.0529	0.034	0.0219	0.0171	0.0452	0.0747	7.4737
Physical security	0.0662	0.028	0.1886	0.0409	0.0744	0.0398	0.1058	0.068	0.1996	0.0282	0.0904	0.0845	8.4595
Regulatory Security	0.0109	0.028	0.1886	0.0409	0.0744	0.0598	0.1604	0.0226	0.0665	0.4284	0.0904	0.1064	10.6496
Security policy	0.1986	0.1683	0.0314	0.1639	0.1861	0.2392	0.2646	0.2062	0.0133	0.0856	0.1356	0.1539	15.3944
Software security	0.1986	0.042	0.0314	0.0204	0.0186	0.0598	0.0529	0.034	0.0332	0.0285	0.0452	0.0513	5.1373

Figure 6.8 All weight values of each perspective after edition.

Figure 6.7 represents weight values before perspective edition. After weight values have been edited successfully, the program will re-calculate all weight values shown in Figure 6.8

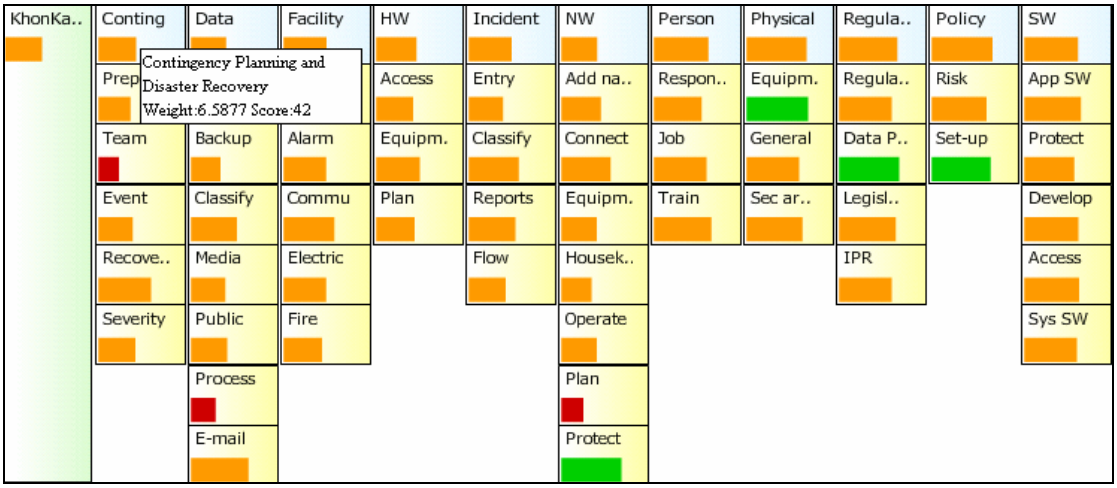

Figure 6.9 Shows the scorecard before editing weight value.

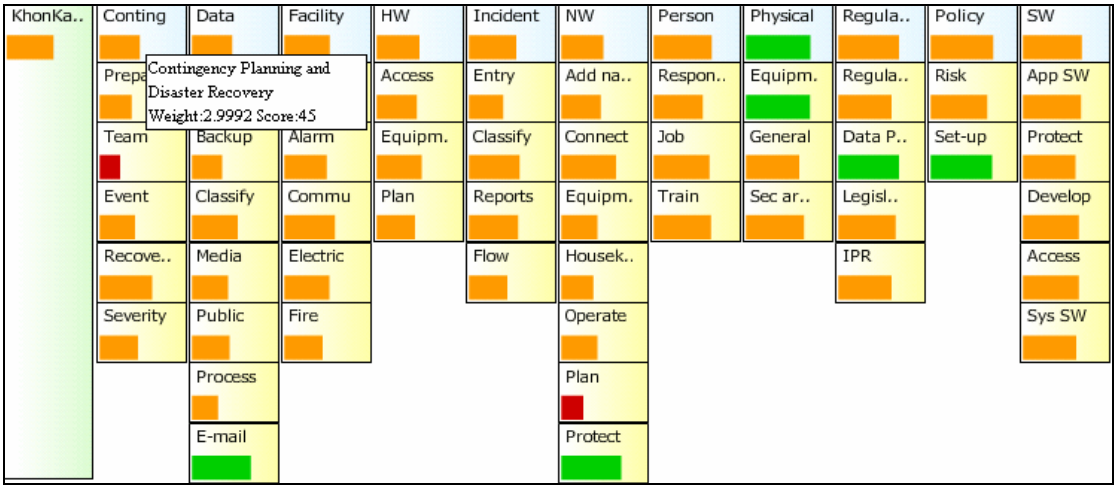

Figure 6.10 Shows the scorecard after editing weight value.

Figure 6.9 displays scorecard before perspective edition and program will recalculate weight and score values after editing the weight values as shown in figure 6.9 and figure 6.10. After edition, the weight of contingency planning changes value from 6.587 to 2.9992 making the score value changes from 42 to 45.

6.1.3 Score assignment

In score assignment of component, user could only define score value of measure by which score values range from 1 to 100. In other components, except measure component, the program will calculate automatically.

6.1.3.1 Initial score

To define the initial scores of each measure which have value ranging from 0 to 100.

Perspective Name	Contingency Planning and Disaster Recovery
Objective Name	Contingency Preparation
Measure Names	**Score**
Resource preparation	0
Site preparation	0

Figure 6.11 Shows the initial score

Figure 6.11 views the screen of initial score displaying the score of ‘Resource Preparation’ and ‘Site Preparation’. Both ‘Resource Preparation’ and ‘Site Preparation’ are measure of ‘Contingency Preparation‘ which is the objective of ‘Contingency Planning and Disaster Recovery’.

6.1.3.2 Score after adjustment

This section describes the score adjustment which the score value can only be adjusted partially at the measure level. After the score adjustment has been done successfully, program will re-calculate the score of objective, perspective, branch, province, region and organization automatically.

Date	06 October 2006
Organization Name	Head Office
Measure	
Name	Score
Resource preparation	75

Figure 6.12 Shows the score value before adjustment.

Date	02 Febuary 2007
Organization Name	Head Office
Measure	
Name	Score
Resource preparation	30

Figure 6.13 Shows the score value after adjustment.

Figure 6.12 represents the score of 'Resource Preparation' before adjustment which has value of 75 and then change to 30 as presented in figure 6.13. The program will re-calculate score of objective, perspective and branch resulting scorecard to be changed as shown in Figure 6.14.

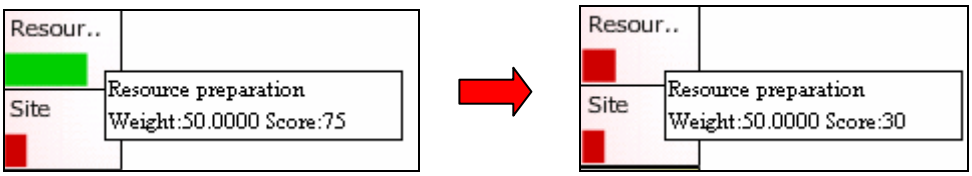

Figure 6.14 Shows the scorecard before and after score adjustment.

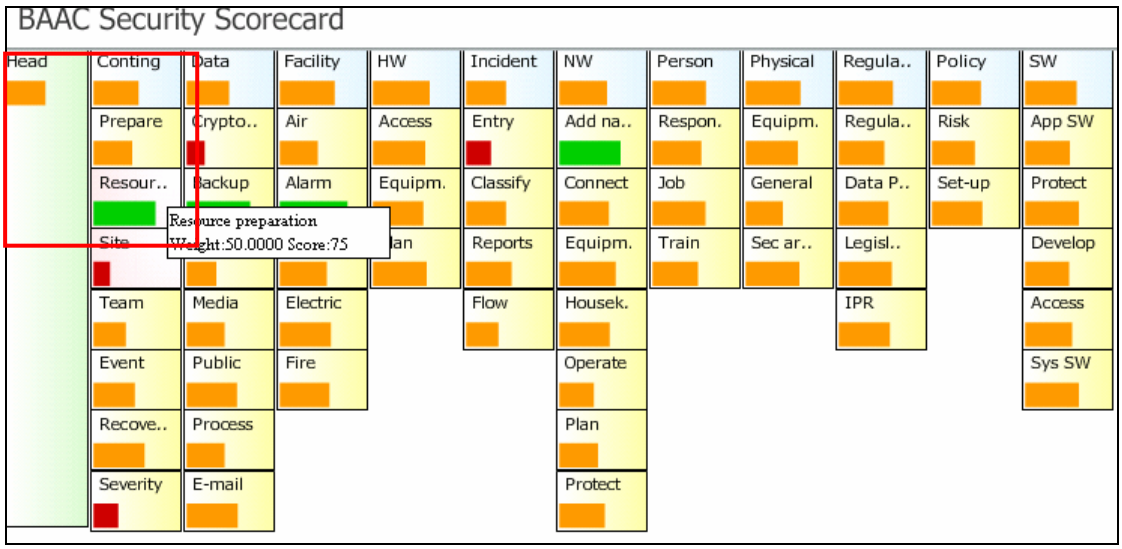

Figure 6.15 Shows the scorecard before score adjustment.

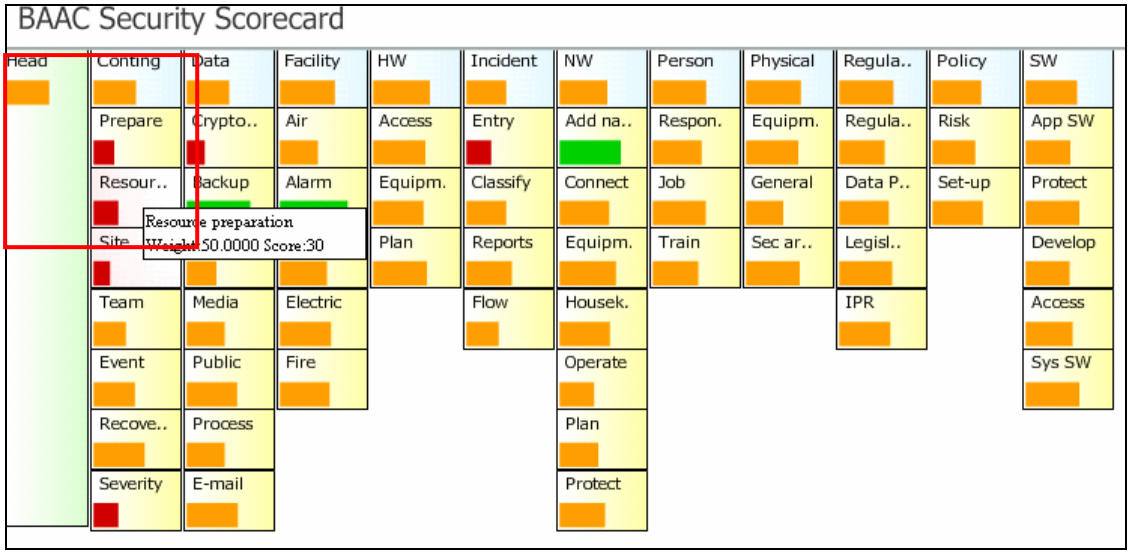

Figure 6.16 Shows the scorecard after score adjustment.

Figure 6.15 shows the scorecard before editing the value of ‘Resource Preparation’. After editing value from 75 to 30, the score value of Score Prepare, Contingency planning and Head will be changed too.

6.2 Scorecard

Scorecard is the methodology to represent assessment results with colors. The results will be evaluated in the following levels, measure, objective, perspective, branch, province, region and organization and will be represented in 2 formats, tree and table.

6.2.1 Security scorecard in a tree form

This screen summarizes the security scorecard in tree format which represents the evaluation results of each node with color, score and weight. Figure 6.17 shows the node description in the table format.

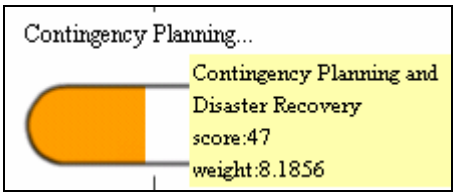

Figure 6.17 Shows the scorecard in tree form.

In tree form, the security scorecard can be divided into 5 levels.

- Security scorecard at the organization level
- Security scorecard at the regional level
- Security scorecard at the provincial level
- Security scorecard at the branch level
- Security scorecard by perspective

6.2.1.1 Security scorecard at the organization level

This screen shows the overall security scorecards at the organization level. We can divide the evaluation result of ICT security into 2 types, overall regional center and branch.

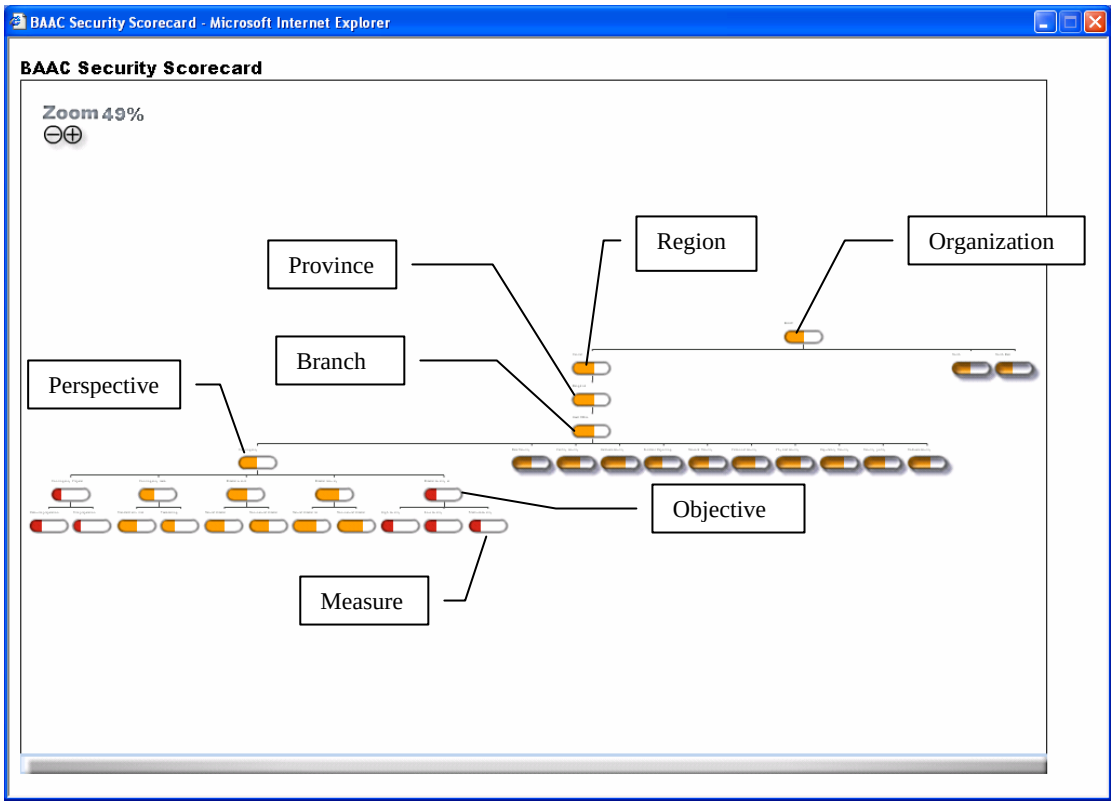

Figure 6.18 The security scorecard of the branch at the organization level in tree form

Figure 6.18 shows the security scorecard of the branch at the organization level which displays the branch located in that province and region. We can divide the security scorecard into 4 parts.

- Branch level shows the ICT security evaluation results from 11 perspectives of each branch.
- Province level shows the average value of ICT security evaluation result of the branch in each province.
- Region level shows the average value of ICT security evaluation result of the province in each region.

- Organization level shows the average value of ICT security evaluation result of all regions.

6.2.1.2 Security scorecard at the regional level

This screen shows the security scorecards at the regional level. The ICT security evaluation results can be divided into 2 types, regional center and branch.

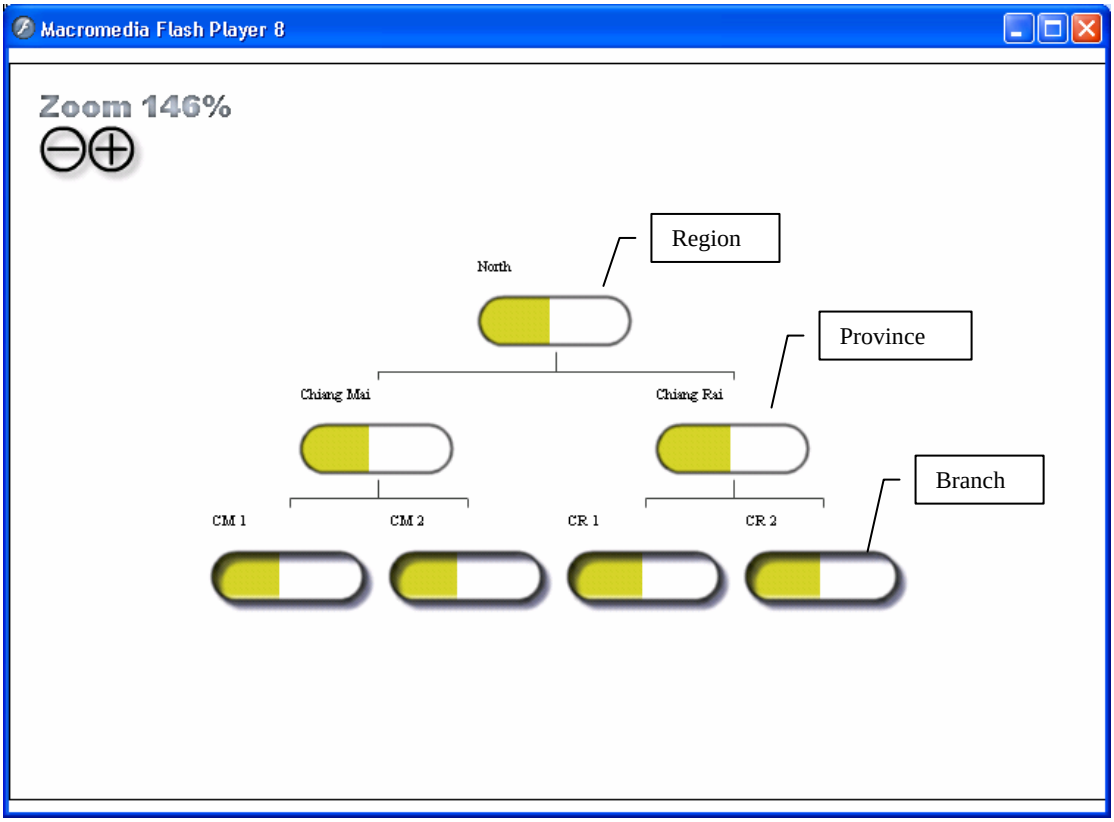

Figure 6.19 The security scorecard of the branch at the regional level in tree form

Figure 6.19 shows the security scorecard of branch at the regional center which displays branches located in that province and region. We can divide the security scorecard into 3 levels.

- Branch level shows the ICT security evaluation results from 11 perspectives of each branch.

- Province level shows the average value of ICT security evaluation result of the branch in each province.
- Region level shows the average value of ICT security evaluation result of the province in each region.

6.2.1.3 Security scorecard at the provincial level

This screen shows the security scorecards at the provincial level by displaying the ICT security evaluation result of each branch located in province.

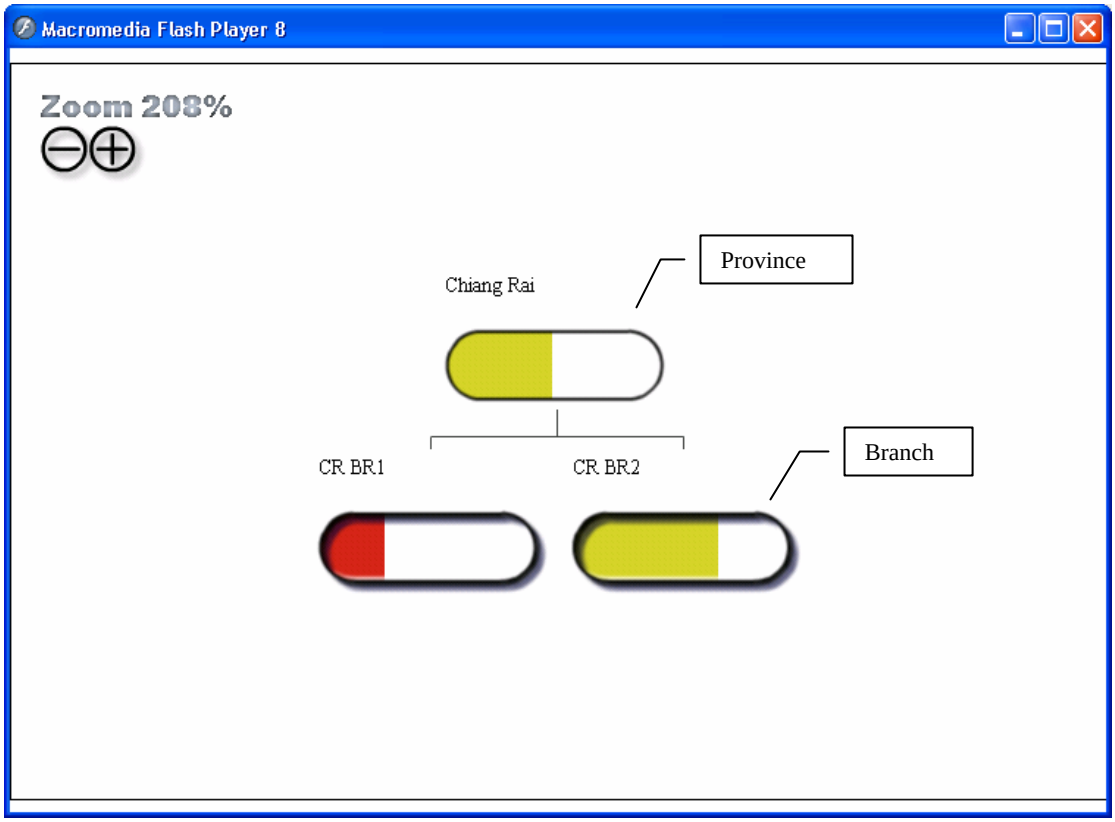

Figure 6.20 The security scorecard of the branch at the provincial level in tree form

Figure 6.20 shows 2 levels of the security scorecard.

- Branch level shows the security scorecard of each branch.
- Province level shows the average value of security scorecard of the branch in province.

6.2.1.4 Security scorecard at the branch level

This screen shows the security scorecard which the ICT security evaluation result can be divide into 3 types, headquarter, regional center and branch.

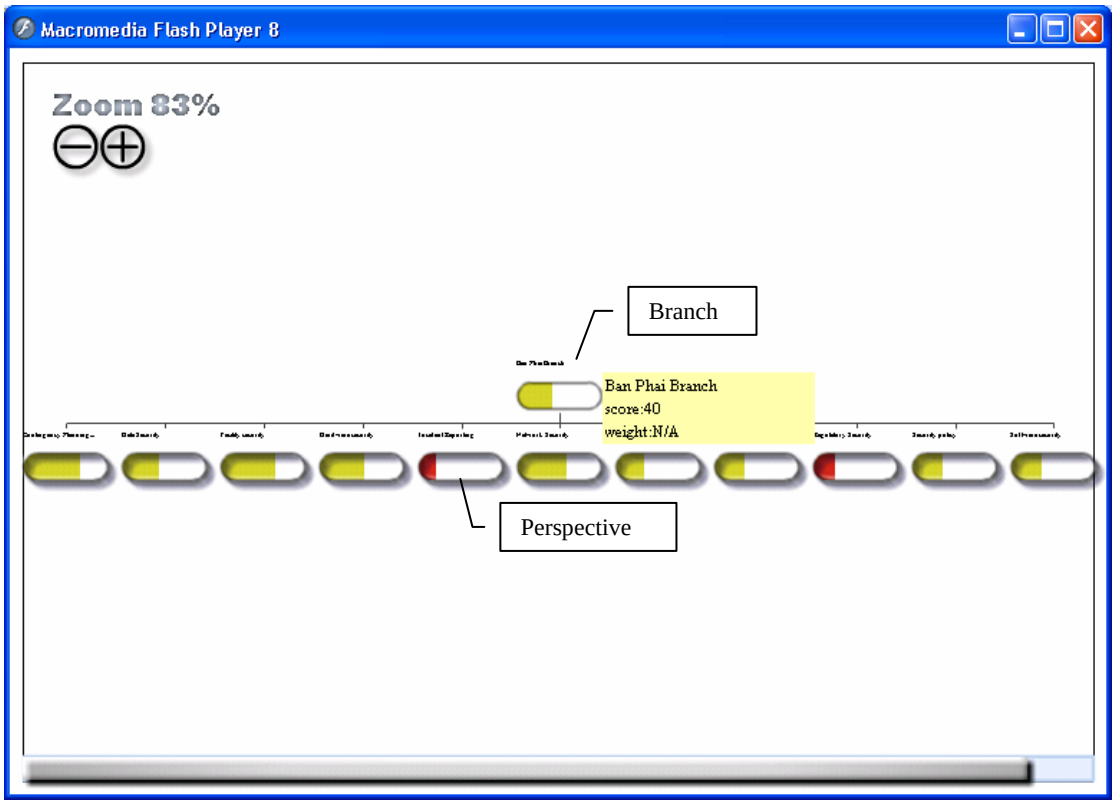

Figure 6.21 The security scorecard of the branch at the branch level in tree form

Figure 6.21 shows the security scorecard of the branch for all 11 perspectives divided into 2 levels.

- Perspective level shows the ICT security evaluation results of each perspective.
- Branch level shows the ICT security evaluation results of the branch.

6.2.1.5 Security scorecard by perspective

This screen shows the security scorecard of 11 perspectives for each branch.

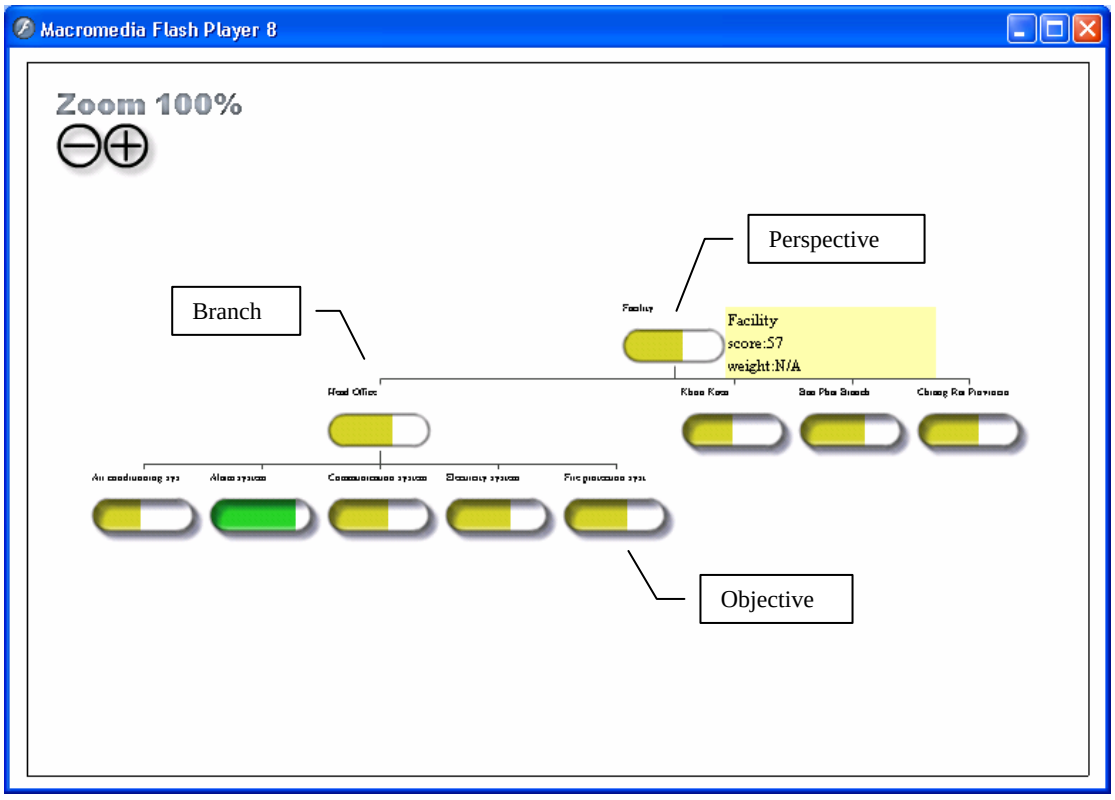

Figure 6.22 The security scorecard by perspective in tree form

Figure 6.22 shows 3 levels of the security scorecards.

- Objective level shows the ICT security evaluation results of each objective.
- Branch level shows the ICT security evaluation result of the perspective for each branch.
- Perspective level shows the average value of ICT security evaluation results for each in the desired perspective.

6.2.2 Security scorecard in a table form

This screen summarizes the security scorecard in table form which represents the evaluation results for each node with color, score and weight. Figure 6.23 shows the node description in the table form.

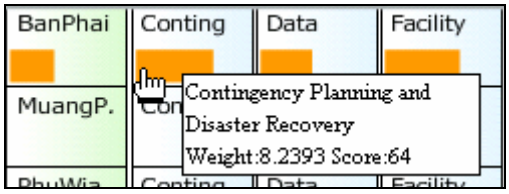

Figure 6.23 shows the scorecard in table form.

We can divide the security scorecard in the table form into 5 levels

- Security scorecard at the organization level
- Security scorecard at the regional level
- Security scorecard at the provincial level
- Security scorecard at the branch level
- Security scorecard by perspective

6.2.2.1 Security scorecard at the organization level

The security scorecard at the organization level can be divided into 2 types, the security scorecard of regional center and branch.

Figure 6.24 The security scorecard of the branch at the organization level in table form

Figure 6.24 shows the security scorecard of branch at the organization level which display branch within province and region. We can divide the table into 5 parts.

- Perspective shows the ICT security evaluation results at the perspective level.
- Branch shows the ICT security evaluation results of branch.
- Province shows the average value of evaluation results of branch in each province.
- Region shows the average value of evaluation results of province in each region.
- Organization shows the average value of evaluation results of all regions.

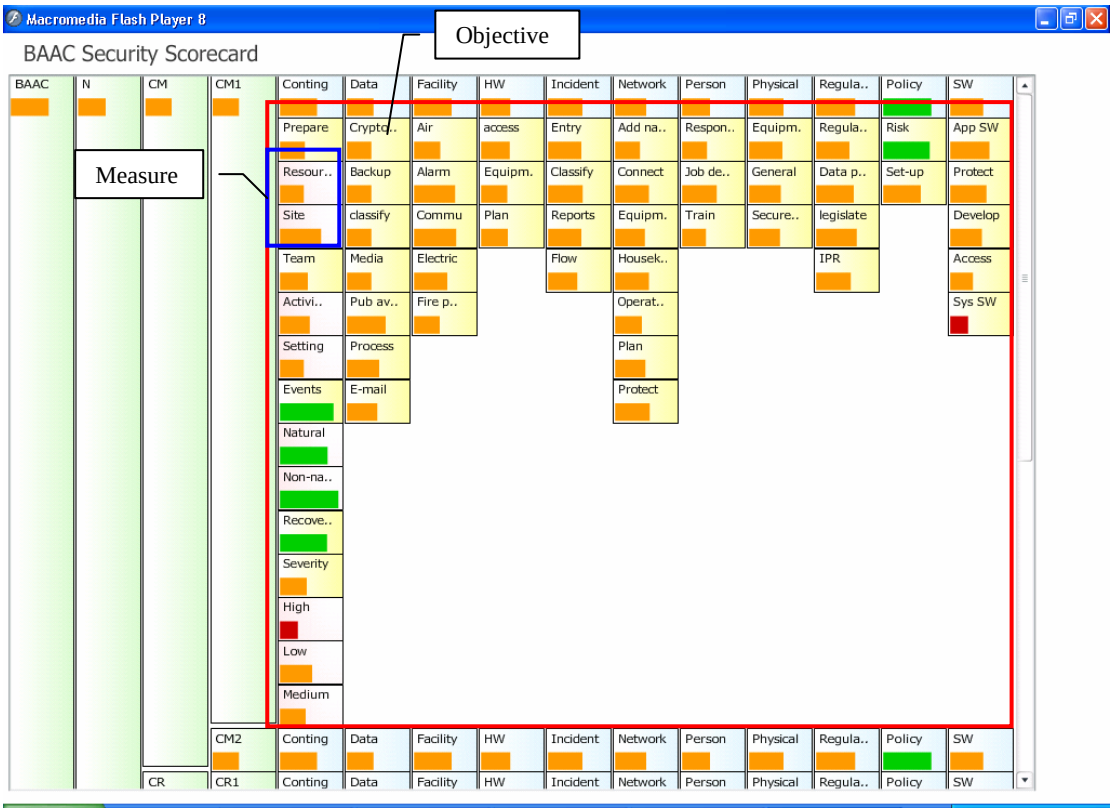

Figure 6.25 The security scorecard of objective and measure of branch at the organization level in table form

System shows the ICT security evaluation results of the objective in each perspective by either clicking “Perspective” node or shows the ICT security evaluation result of the measure by clicking “Objective” node as shown Figure 6.25.

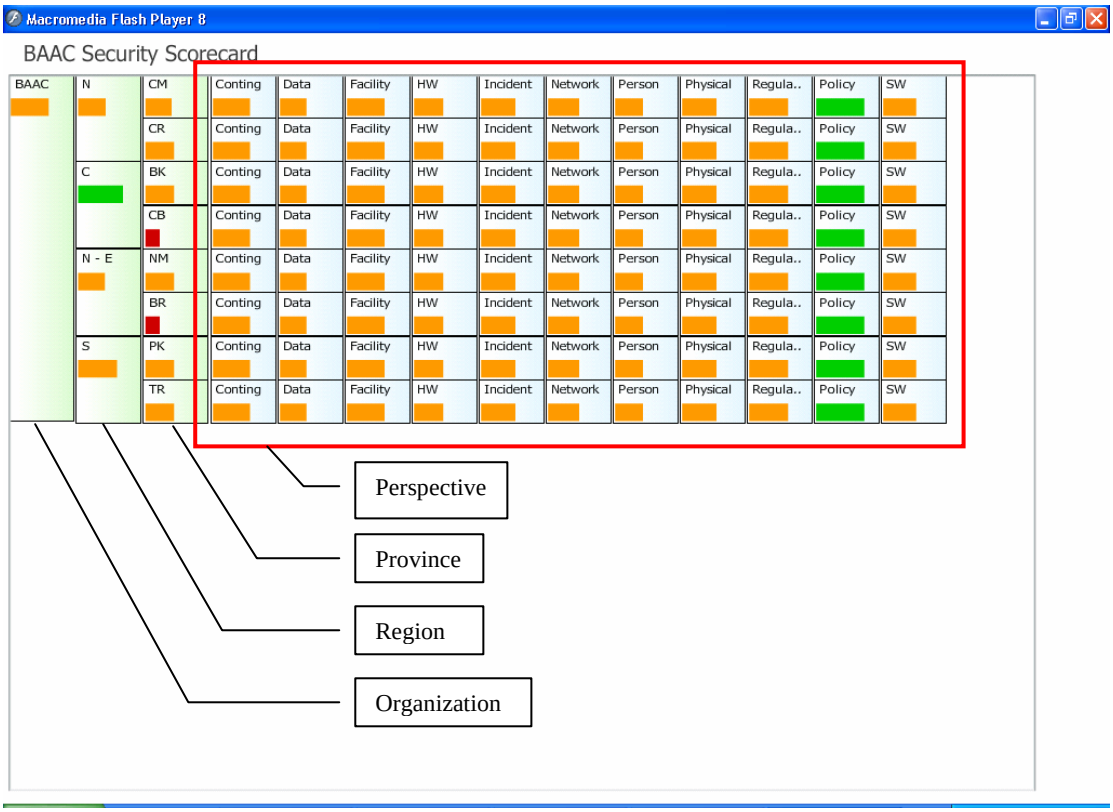

Figure 6.26 The security scorecard of province at the organization level in table form

System shows the ICT security evaluation result of each province by clicking “Province” node as shown Figure 6.24. Figure 6.26 shows the ICT evaluation results of each province in table format divided into 4 parts.

- Perspective shows the average value of evaluation results at the perspective level in each branch.
- Province shows the average value of evaluation results of all branches in each province.
- Region shows the average value of evaluation results of all regional centers in each region.
- Organization shows the average value of evaluation results of all regions.

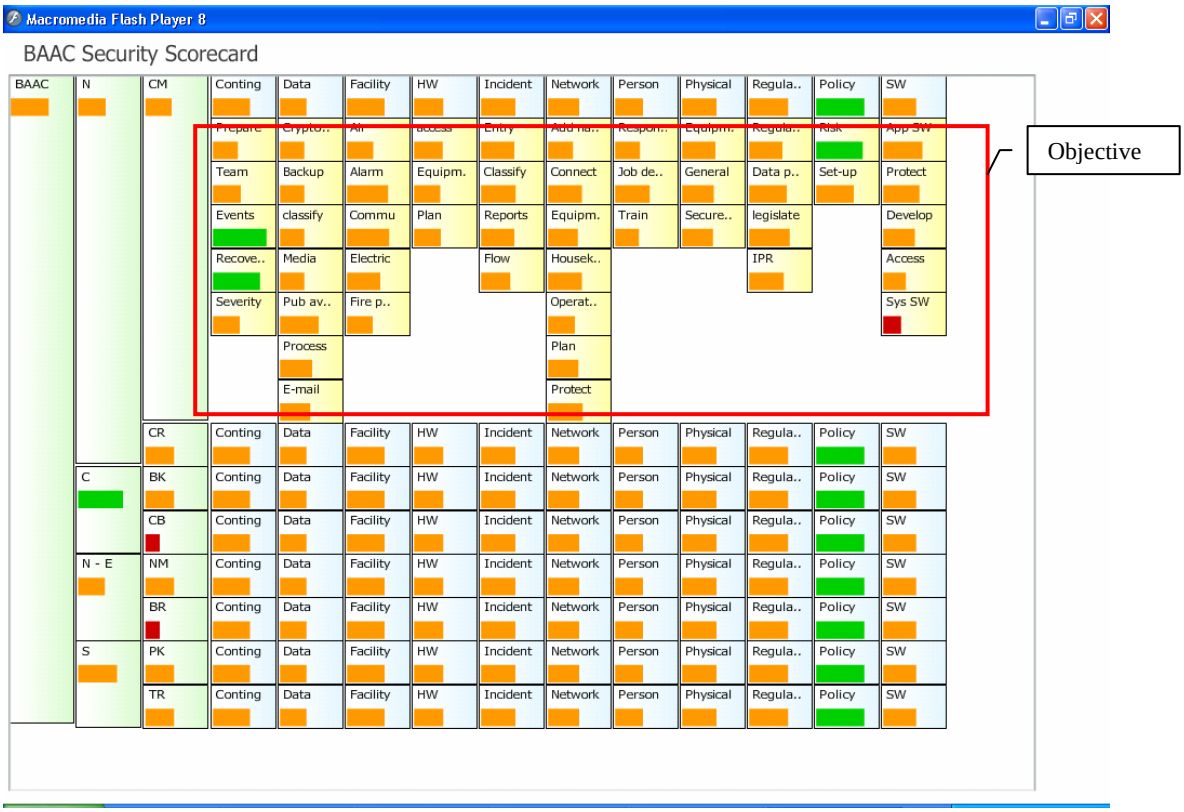

Figure 6.27 The security scorecard of objective of province at the organization level in table form

When users click at “Perspective” node in Figure 6.24, system will show the ICT security evaluation results of the objective in each perspective and show the ICT security evaluation results of the measure in each objective by clicking “Objective” node as shown in Figure 6.27.

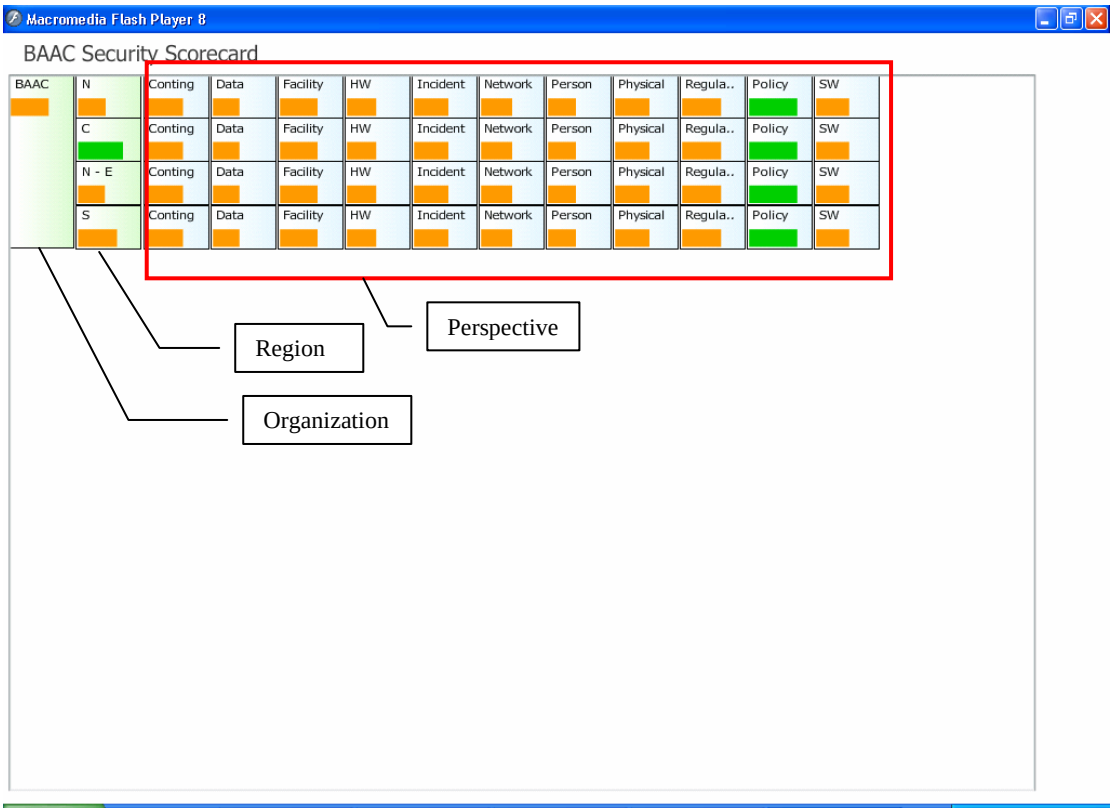

Figure 6.28 The security scorecard of region at the organization level in table form

When users click at “Region” node in Figure 6.24, system will show the ICT security evaluation results of the region as shown in Figure 6.28 that the table is divided into 3 parts.

- Perspective shows the average value of evaluation results at the perspective level of each region.
- Region shows the average value of evaluation results of the regional center in each region.
- Organization shows the average value of evaluation results of all regions.

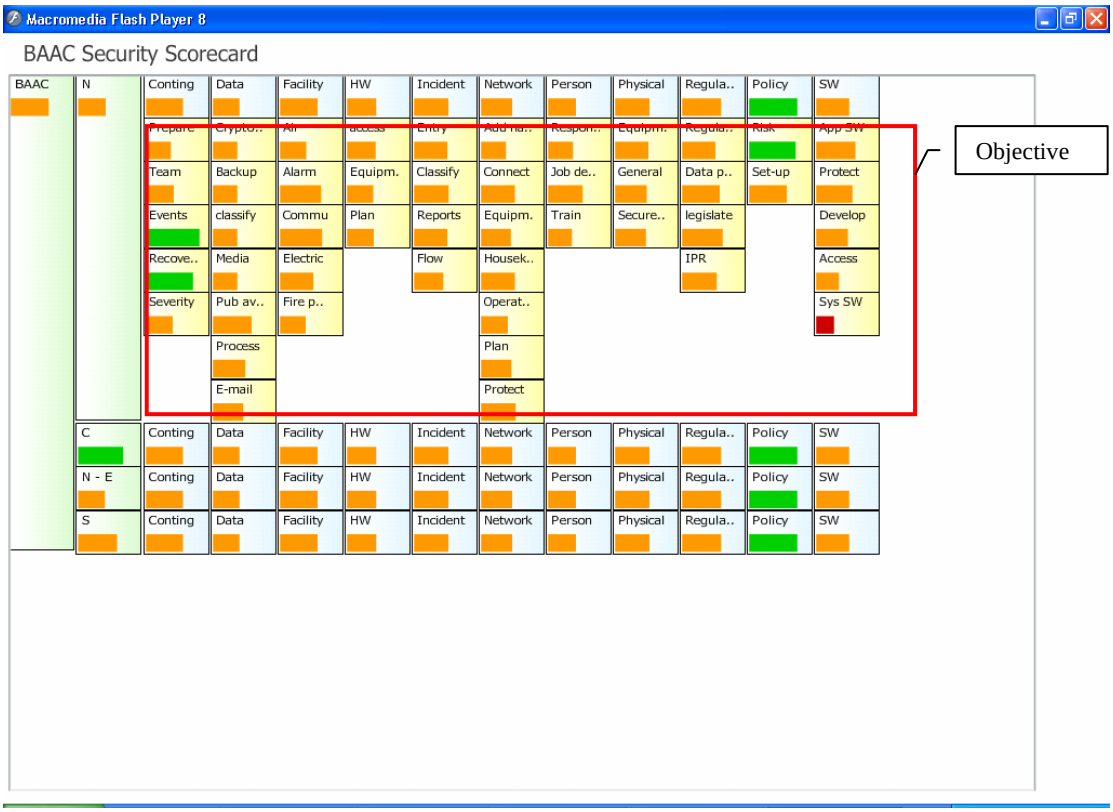

Figure 6.29 The security scorecard of objective of region at the organization level in table form

When users click at “Perspective” node in Figure 6.28, system will show the ICT security evaluation results of the objective in each perspective and will show the ICT security evaluation results of the measure in each objective by clicking “Objective” node as depicted in Figure 6.29.

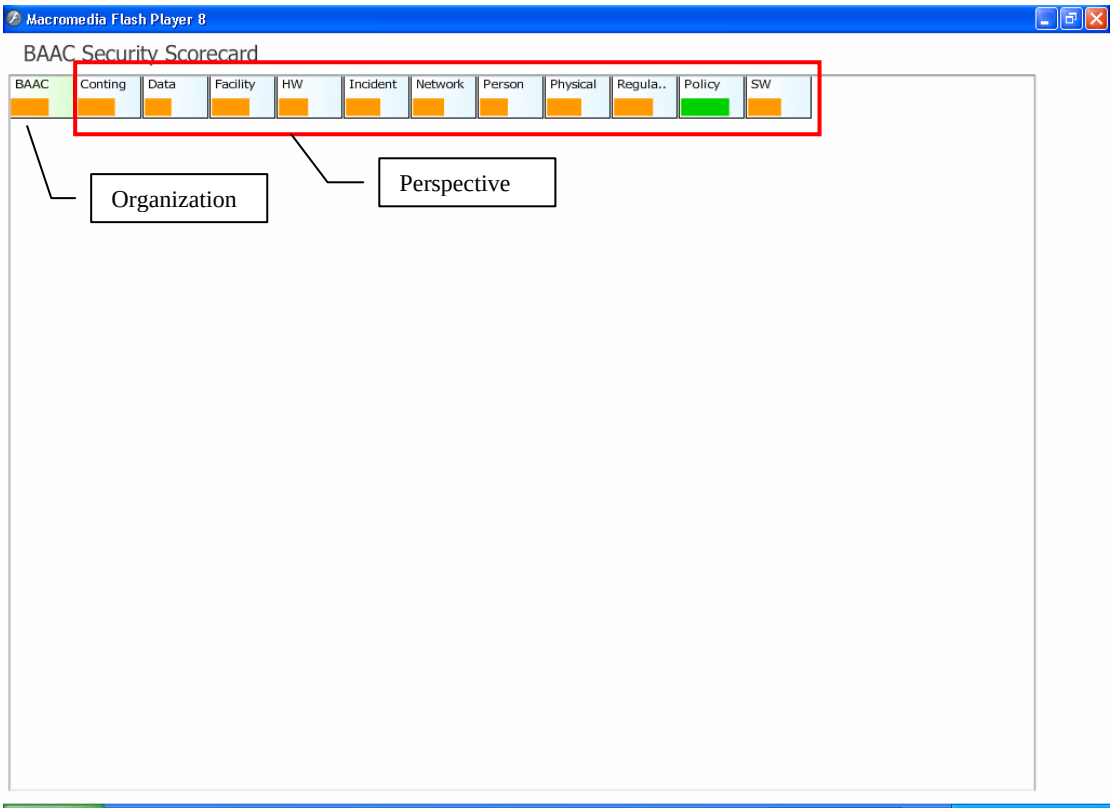

Figure 6.30 The security scorecard of organization at the organization level in table form

When users click at “Organization” node in figure 6.24, system will show the ICT security scorecard evaluation results of the organization as illustrated in figure 6.30 which the table is divided into 2 parts.

- Perspective shows the average value of evaluation results at the perspective level in the organization.
- Organization shows the average value of evaluation results of the organization.

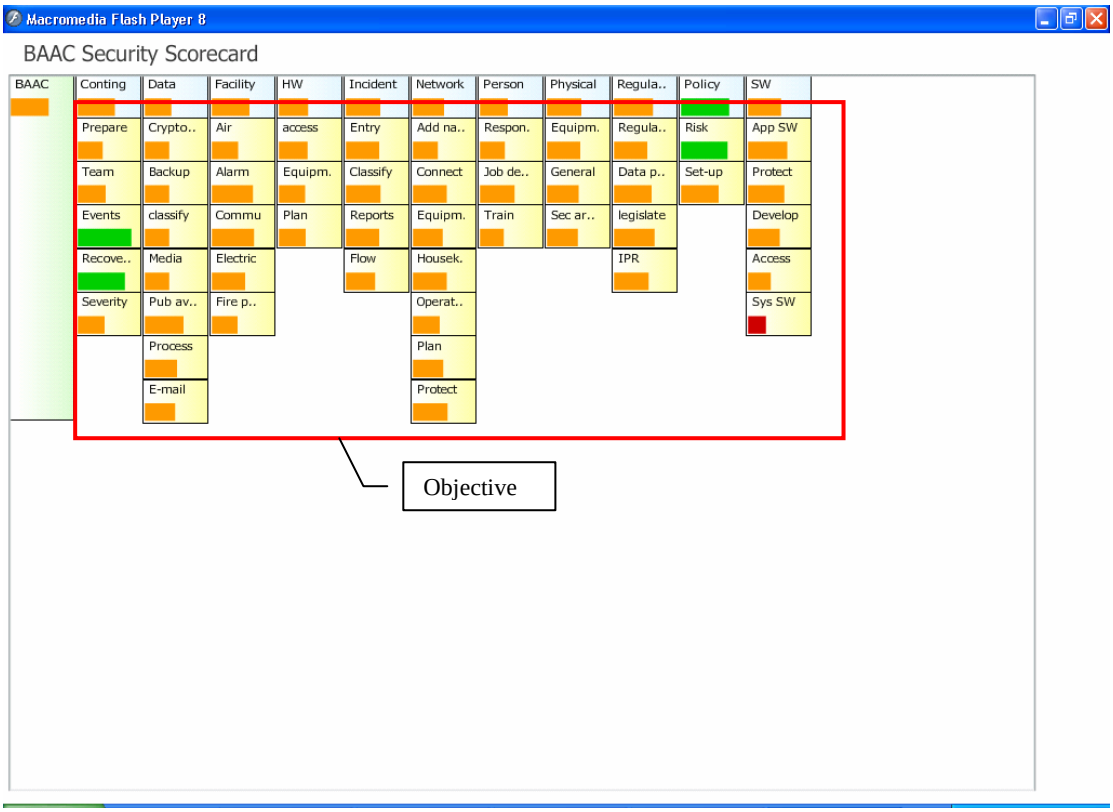

Figure 6.31 The security scorecard of objective of organization at the organization level in table form

When users click at “Perspective” node in Figure 6.30, system will show the ICT security evaluation results of the objective in each perspective and will show the ICT security evaluation results of the measure by clicking “Objective” node as shown in Figure 6.31.

6.2.2.2 Security scorecard at the regional level

This screen shows the ICT security scorecard at the regional level and summarizes the ICT security evaluation results in each region by dividing results into 2 parts, the ICT security evaluation result of all regional centers and all branches.

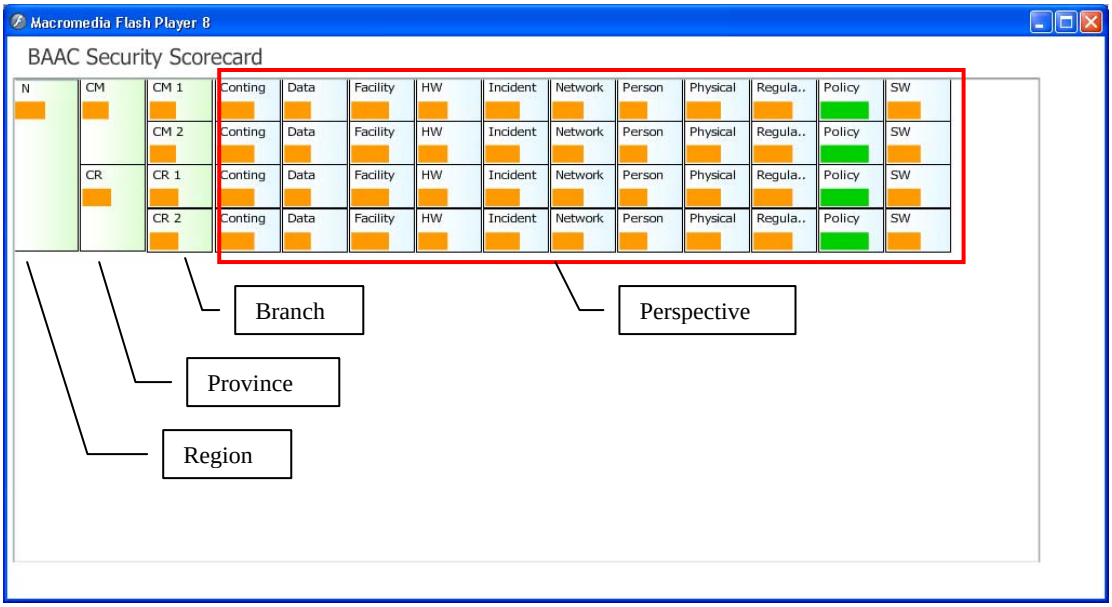

Figure 6.32 The security scorecard of branch at the regional level in table form

Figure 6.32 shows the security scorecard of the branch in the region perspective displaying the ICT security evaluation results of branch within its province and region. This screen can be divided into 4 parts.

- Perspective shows the ICT security evaluation results at the perspective level of each branch.
- Branch shows the ICT security evaluation results of the branch.
- Province shows the average value of ICT security evaluation results of the branch in the province.
- Region shows the average value of ICT security evaluation results of the province in the region.

When users click at “Perspective” node, system will show the ICT security evaluation results of the objective in each perspective or will show the ICT security evaluation results of the measure in each objective by clicking “Objective” node. By clicking “Province” or “Region” node, system will show the ICT security evaluation results of the province or region of each perspective. When users click at “Perspective” node, system will show the ICT security evaluation results of the objective and will show the ICT security evaluation results of the measure by clicking “Objective” node with same manner as the security scorecard at the organization level.

6.2.2.3 Security scorecard at the provincial level

This screen shows the ICT security scorecard at the provincial level which summarizes the ICT evaluation results of all branches. The security scorecard of the province shows the average value of the ICT security of all branches in each region.

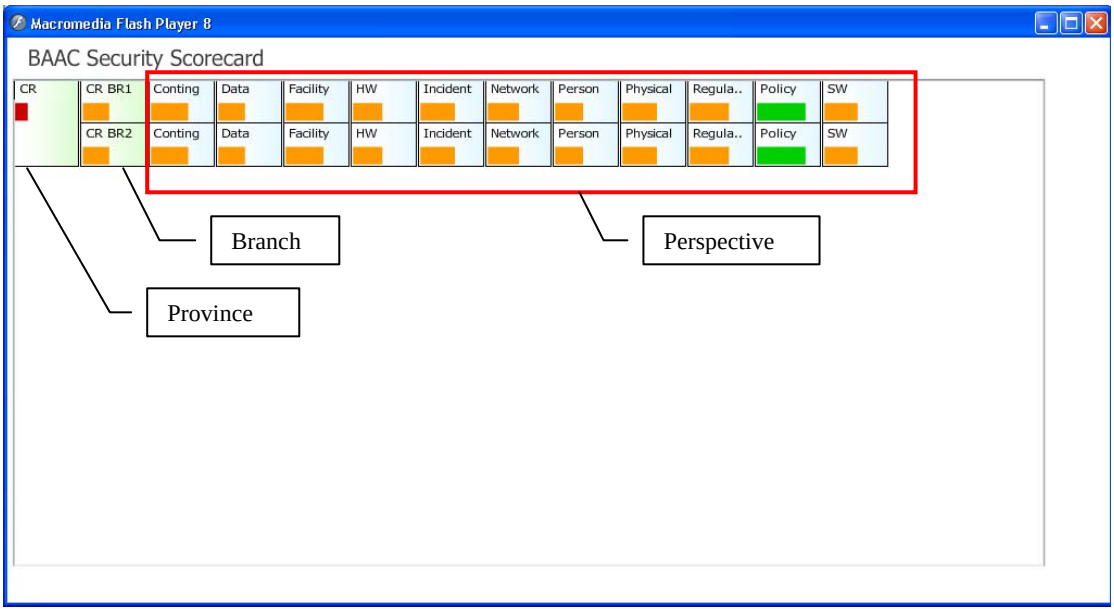

Figure 6.33 The security scorecard of branch at the provincial level in table form

Figure 6.33 shows the scorecard of branch in the province perspective which the table can be divided into 3 parts.

- Perspective shows the ICT security evaluation results at the perspective level of each branch.
- Branch shows the ICT security evaluation results of the branch.
- Province shows the average value of ICT security evaluation results of branch in the province.

When users click at “Perspective” node, system will show the ICT security evaluation results of the objective in each perspective or clicking “Objective” node, system will show the ICT security scorecard evaluation results of the measure in each objective.

By clicking “Province” node, system will show the ICT security evaluation results of province by each perspective or clicking “Perspective” node system will show the ICT security evaluation results of the objective. When users click at “Objective” node system will show the ICT security evaluation results of the measure with the same manner as the security scorecard at the organization level.

6.2.2.4 Security scorecard at the branch level

This screen shows the security scorecard of each branch summarizing the ICT security evaluation into 3 types of branch, headquarter, regional center and branch.

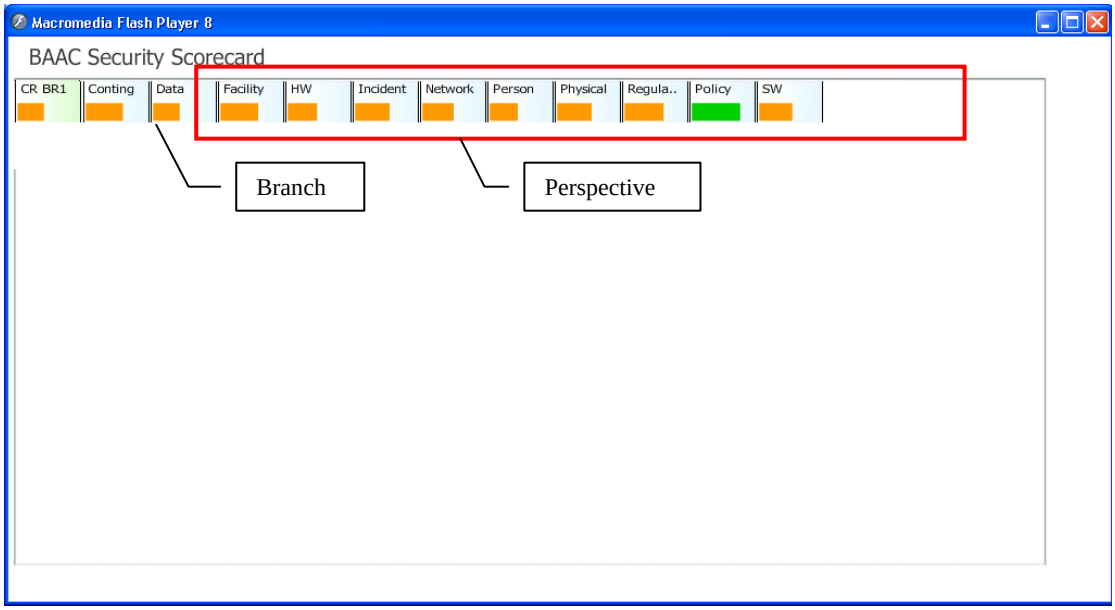

Figure 6.34 The security scorecard of branch at the branch level in table form

Figure 6.34 shows the security scorecard of the branch which displays all 11 perspectives that the table is divided into 2 parts.

- Perspective shows the ICT security evaluation result at the perspective level of the branch.
- Branch shows the ICT security evaluation result of the branch.

When users click at “Perspective” node, system will show the ICT security evaluation results of the objective in each perspective or clicking “Objective” system will show the ICT security evaluation of the measure in each objective displaying all information in the same format as the security scorecard at the organization level.

6.2.2.5 Security scorecard by perspective

This screen shows the security scorecard of the perspective at the branch level that displays all information of each perspective.

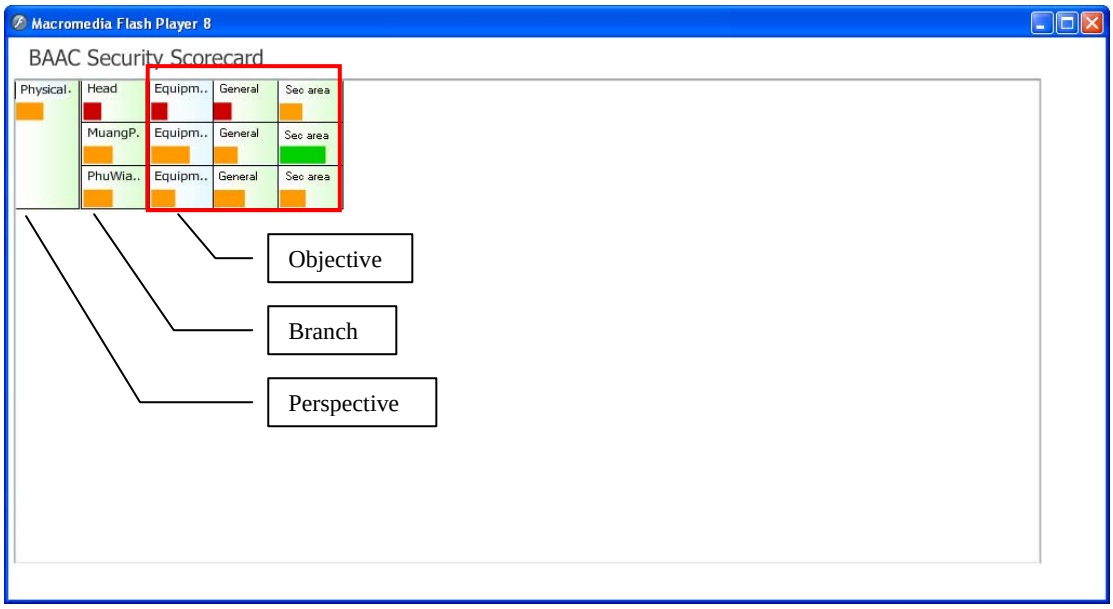

Figure 6.35 Security scorecard by perspective in table form

Figure 6.35 shows the security scorecard of the perspective at the branch level which the table can be divided into 3 parts.

- Objective shows the ICT security evaluation results at the objective level in each branch.
- Branch shows the ICT security evaluation results at the perspective level in each branch.
- Perspective shows the average value of ICT security evaluation results at the perspective level in each branch.

System shows the ICT security evaluation results of the measure in each objective by clicking "Objective" that displays all information as same as the security scorecard at the organization level.

CHAPTER VII
DISCUSSION AND CONCLUSION

This chapter makes a discussion on the research project development and also makes a conclusion of a system of the ICT security efficiency measurement of an organization.

7.1 Discussion

This section discusses the system limitation, system performance, resource utilization and error factors of evaluation.

7.1.1 System limitation

The development of the system of the ICT security efficiency measurement of an organization for this research project uses Bank for Agriculture and Agricultural Cooperatives (BAAC) as a case study. Currently, BAAC has 567 branches, exclusive of its provincial offices, Islam Bank Fund, Micro branches, district units and business units. ICT is apparent that there is an inordinate number of the Bank's branches. For this prototype, the number of branches is limited to 100, which is within its support. Each branch is under the supervision of provinces and regions, based on the Bank's organizational structure. Consequently, the system limitation is defined with the following details.

- The system divides indicators for the ICT security efficiency measurement into 3 levels of perspective, objective and measure.

- For one branch, the system can support 11 perspectives used for measurement. The 11 aspects (perspectives) of security are gathered from the International Standard ISO/IEC 17799.

- Based on the organization's structure, a branch is under the province to which it is attached. For this research project, it is defined that for one province, the system can support 10 branches.

- Based on the organization's structure, a province is under the region to which it is attached. For this research project, it is defined that for one region, the system can support 10 provinces.

- Based on the organization's structure, a region is under the supervision of the organization. For this research project, it is defined that for one organization, the system can support 4 regions.

It is worth noting that if the system is to be applied to a large organization, the appropriate number of branches should be increased so that the system can support them.

7.1.2 System performance

Based on the experimental consequence, the system performance on a display of the result of the ICT security efficiency measurement of the organization in the form of a scorecard consists of the following detail.

- Security scorecard at the organizational level takes the average time of 36.66 seconds to display the result.

- Security scorecard at the regional level takes the average time of 7.17 seconds to display the result.

- Security scorecard at the provincial level takes the average time of 5.97 seconds to display the result.

- Security scorecard at the branch level takes the average time of 5.47 seconds to display the result.

- Security scorecard by perspective takes the average time of 5.74 seconds to display the result.

It is noted that the time spent on displaying an outcome may change according to the amount of data. Provided that one needs to speed up the display time, a method of display should be modified. In this research project, since the outcome is presented in the form of flash, it takes quit a lot of time to display the result because the XML has to be generated and a flash file established in order to display the result on web.

7.1.3 Resource utilization

To setup the prototype of the system of the ICT security efficiency measurement of the organization, we need a computer installed with Apache Tomcat Server 4.1, Java(TM) 2 SDK, Standard Edition 1.4.2_03, Macromedia Flash Player 8, Microsoft SQL Server 2000, and Source code of the system of ICT security efficiency measurement of the organization. When the system is run, a total resource of 79.18 MB is utilized, of which the detail is revealed in Table 7.1.

Program	Memory usage
Java	45.27 MB
Microsoft SQL Server 2000	9.6 MB
Internet Explorer	24.31 MB

Table 7.1 Memory usage

7.1.4 Error factors of evaluation

The consequence of the ICT security efficiency measurement of the organization stems from a calculation of the score and weight of indicators. Typically, to define the score and weight is difficult since there is no certain standard or criterion for defining. Therefore, to define all necessary parameters relies on an evaluator, making the evaluation consequence based on each organization’s measurement criteria (measure).

For the development of the system of the ICT security efficiency measurement of an organization in this research project, the weight is defined based on an evaluator

of each branch. Virtually, an evaluator has to defined the significance value of each indicator used for a measurement while he/she, in each branch, normally has different viewpoints and no definite criteria for defining the significance value. As a consequence, the weight received is, more often than not, unrealistic. Similarly, it is also hard to define realistic scores of measures (criteria) for different branches due to different opinions of evaluators, who give scores based on their viewpoint.

7.2 Conclusion

In chapter 2 the objectives and scope of the development of the system of the ICT security efficiency measurement of an organization are discussed. After the system development and experimentation, it is found that the system can achieve the objectives defined. This means that it can measure the efficiency of the ICT security of the Bank's branches, regional centers, provinces, regions and the Bank (organization) itself. Furthermore, it can also display the measurement consequence in two forms of scorecards, namely, tree and table.

REFERENCES

1. Clemens L, Leonard F, Marc W. Designing a performance measurement system: a case study. Elsevier B.V. 2003.
2. Chenxi W, William A. Towards a framework for security measurement. University of Virginia 1997.
3. Erkan K. Evaluating IT security performance with quantifiable metric. Institutionen for Data-och Systemvetenskap 2005.
4. Heinz A. Applying the balanced scorecard concept: an experience report. Elsevier Science Ltd. 2001.
5. International Standard ISO/IEC 17799. Information technology – code of practice for information security management. BSI; 2001.
6. John M. Security measurement. PSM Security Measurement 2004.
7. Koen M, Roger M. The use of the balanced scorecard for the evaluation of information and communication technology projects. Elsevier Science Ltd. 2004.
8. Marlys G, Steven S. A note on the judgmental e.ects of the balanced scorecard's information organization. Elsevier Science Ltd. 2002.
9. Richard H. Guide to a balanced scorecard performance management methodology. Procurement Executives' Association 1999.
10. Robert K, David N.The balanced scorecard measures that drive performance. Harvard Business Review; 1992 Jan-Feb. p.70-80.
11. Rodney S, Sherif M. Evaluating the value IT adds to the process of project information management in construction. Elsevier Science B.V. 2003.
12. Stan D, Tom A. An investigation of the effect of balanced scorecard implementation on financial performance. Elsevier Science Ltd. 2004.

13. Tariq D, Sheila F, Allan C. Extending the balanced scorecard for technology strategy development. IEEE 2000.
14. Volkmar H. Computer models for strategic business process optimization. IEEE 2000.
15. Wim V, Ronald S. Aligning business and information technology through the balanced scorecard at a major canadian financial group: its status measured with an IT BSC maturity model. IEEE System Sciences 2001.

BIOGRAPHY

NAME Miss Orathai Ungamrung

DATE May 28, 1979

PLACE OF BIRTH Bangkok, Thailand

INSTITUTIONS ATTENDED Prince of Songkla University, 1999-2002:
Bachelor of Science (Computer Science)

Mahidol University, 2003-2006:
Master of Science (Computer Science)

POSITION & OFFICE 2005 – Present,
Freewill Solutions Company Limited,
Thailand
Position: Senior Project Developer

2003 – 2005,
Computing Center, Mahidol
University, Bangkok, Thailand
Position: System Analyst