The Information Systems Security Training Program: A work in progress

Asım Gençer Gökce
TUBITAK-BILGEM-Cyber Security Institute
Ankara, Turkey

Yılmaz Çankaya
TUBITAK-BILGEM-Cyber Security Institute
Gebze, Turkey

Abstract—**The high cost of information security breaches increases the importance of information security for all organizations. The organizations need to educate their employees in order to protect their information assets. Public enterprises and governmental organizations that provide information services to citizens need to protect their services. This paper reports on the use of design-based research [1] as an approach to develop an information systems security program for public enterprises and governmental organizations in Turkey. This paper focuses on the current state of the Information Systems Security Training Program.**

Information security, information security training, security education, design-based research

I. Introduction

The organizations use the Internet and private networks for communication, and they use firewalls, virtual private networks, attack detection / prevention systems, anti-virus systems, content filtering software, authentication mechanisms, and authorization systems to protect their information assets. It is criticized by Stanton [2] that the organizations mainly focus on technical and procedural security measures, ignoring the human dimension of information security. The information security breaches affect not only the information systems but also everyone [3] using the system. The public enterprises and governmental organizations that provide major information services to users are also the major target of information system abusers. Thus they need to educate their system administrators and users in order to avoid information security breaches.

The human factor has become an important topic in information systems and information security research [4] [5]. From an educational point of view, information security training programs mainly lack theoretical background. The studies of Aytes and Connolly [6] revealed that current information security approaches do not ensure positive acquisitions for education since they do not have scientific fundamentals. Our proposed program is developed by a design-based approach to satisfy theoretical and scientific foundations.

II. Design-Based Research

Design-based research offers valuable insight into the development of educational programs. Wang and Hannafin [7] defined design-based research as an iterative process of analysis, design, development and implementation to enhance educational practices involving researchers and participants in a real world setting. The aim of design-based research is to produce design principles and information to enhance solutions for educational problems.

Due to the analysis, design, development and evaluation nature of the proposed program, the principles of developmental research will be followed during the study. The framework for this research is based on the design-based research approach, which is conceptualized by Reeves at Figure 1 [1], and the whole Public Information Systems Security Program (PISSP) is examined in the four iterative phases set out in Figure 1. What follows is a brief description of what will occur within each of these phases with an explanation of how design-based research aims to satisfy the overall objective of developing an information systems security program.

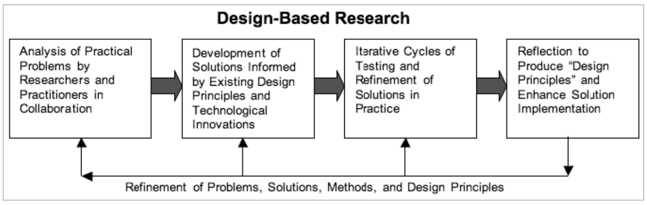
Design-Based Research
Analysis of Practical Problems by Researchers and Practitioners in Collaboration
Development of Solutions Informed by Existing Design Principles and Technological Innovations
Iterative Cycles of Testing and Refinement of Solutions in Practice
Reflection to Produce "Design Principles" and Enhance Solution Implementation
Refinement of Problems, Solutions, Methods, and Design Principles

Figure 1. Design Based Research Approach [1]

The iterative cycles of data collection and analysis enable the researchers to revise the design principles and the developed program based on the collected data.

III. Design

TRAINING PROJECT: The Information Security Certification Program (ISCP) will be developed by the design-based research approach. The project will be conducted following the four iterative phases. In the first phase, the scope of the ISCP will be identified. Then, the draft of the ISCP will be developed in the second phase. In the third phase, the draft program will be revised by two iterative processes by conducting the first and second phases consecutively. In the final phase, the final version of ISCP will be implemented by the participating organization. The overview of the Training Project is given in Figure 2.

This work is sponsored by The Turkish Ministry of Development under the Information Systems Security Program for Government Organizations.

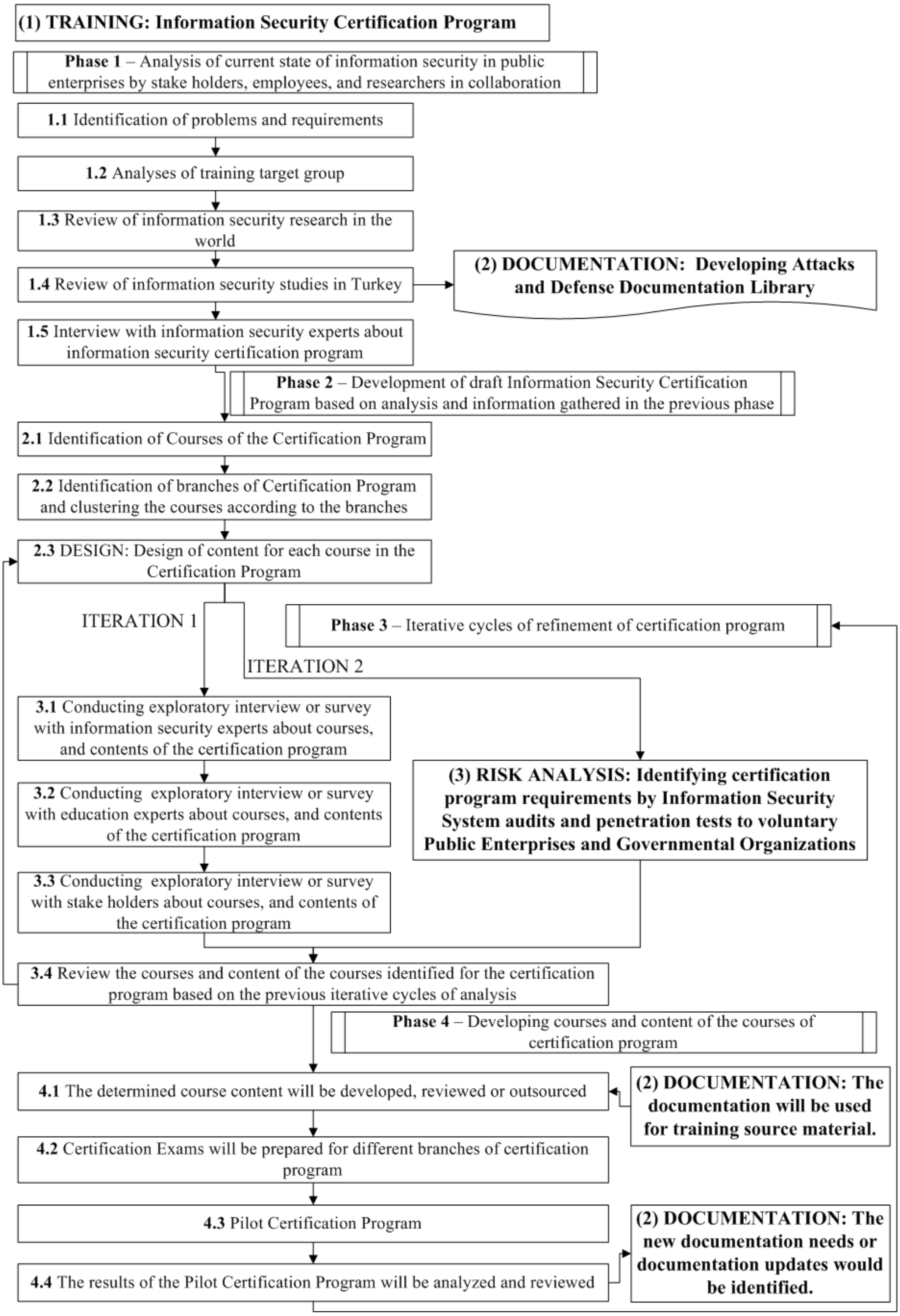
(1) TRAINING: Information Security Certification Program
Phase 1 – Analysis of current state of information security in public enterprises by stake holders, employees, and researchers in collaboration
1.1 Identification of problems and requirements
1.2 Analyses of training target group
1.3 Review of information security research in the world
1.4 Review of information security studies in Turkey
(2) DOCUMENTATION: Developing Attacks and Defense Documentation Library
1.5 Interview with information security experts about information security certification program
Phase 2 – Development of draft Information Security Certification Program based on analysis and information gathered in the previous phase
2.1 Identification of Courses of the Certification Program
2.2 Identification of branches of Certification Program and clustering the courses according to the branches
2.3 DESIGN: Design of content for each course in the Certification Program
ITERATION 1
ITERATION 2
Phase 3 – Iterative cycles of refinement of certification program
3.1 Conducting exploratory interview or survey with information security experts about courses, and contents of the certification program
3.2 Conducting exploratory interview or survey with education experts about courses, and contents of the certification program
3.3 Conducting exploratory interview or survey with stake holders about courses, and contents of the certification program
(3) RISK ANALYSIS: Identifying certification program requirements by Information Security System audits and penetration tests to voluntary Public Enterprises and Governmental Organizations
3.4 Review the courses and content of the courses identified for the certification program based on the previous iterative cycles of analysis
Phase 4 – Developing courses and content of the courses of certification program
4.1 The determined course content will be developed, reviewed or outsourced
(2) DOCUMENTATION: The documentation will be used for training source material.
4.2 Certification Exams will be prepared for different branches of certification program
4.3 Pilot Certification Program
4.4 The results of the Pilot Certification Program will be analyzed and reviewed
(2) DOCUMENTATION: The new documentation needs or documentation updates would be identified.

Figure 2. Overview of Study Design

A. Phase 1: Analysis of practical problems by researchers and practitioners in collaboration

1) Analysis of Current Status of Public Enterprises and Governmental Organizations

The first phase of the Training Project will provide information for the Risk Analysis and Documentation Project. The data gathered in this phase will help the researchers to determine the necessary documentation and required system tests in the risk analysis project.

In order to design an information security certification program for public organizations, the current status of public enterprises and governmental organizations will be analyzed by researchers and employees of these organizations. The surveys and questionnaires will be provided to managers and employees at public enterprises and governmental organizations in order to identify information security problems and requirements. The aim of the surveys will be to gather information about cyber-security threats, security incidents, incident reports and previous information security training background of the organizations.

2) Analysis of ISCP Target Group

In order to determine the target group profile of ISCP, the information about employees' information technology and information security proficiencies, demographic data, and educational backgrounds of public enterprises and governmental organizations will be identified.

3) Information Security Studies in the World

The information security trends in the world will be the major determinant in the development of the information security certification program. Thus, the security reports of major security companies and reports of Computer Emergency Response Teams (CERTs) all over the world will form the base of security trends in the world. In addition, the information security programs of private organizations and universities will be analyzed according to their course content.

4) Information Security Studies in Turkey

The second major determinant of the development of the information security certification program will be the current status of information security and information security education in Turkey. In order to gather information about the current status, the security incidents and notifications reported to the Turkish Computer Emergency Response Team (TR-CERT) will be analyzed.

Additionally, the results of the National Cyber Security Exercise 2011 [8] final report will contribute to the identification of security trends in Turkey. For instance, last years' report will provide valuable insights for the information security requirements in Turkey. Moreover, the information security programs of private organizations and universities in Turkey will be compared with the courses and their content.

The courses and their content of the ISCP will be based on the analysis of public enterprises and governmental organizations, information security studies and trends in the world and Turkey. The information security experts will be asked to review the developed information security certification program. The data gathered in this phase and the analysis conducted will form the basis of the Documentation Project (Attacks / Defense Documentation Library), which is the second project of the proposed program.

B. Phase 2: Development of solutions supported by existing design principles and technological innovations

Draft ISCP will be developed based on the analyses, information gathered, and review of information security experts. In this phase, different types of certification programs will be identified and the courses will be categorized as pre-requisite, must or elective course. The courses will be developed according to the contents identified in the previous phases.

C. Phase 3: Iterative cycles of testing and refinement of solutions in practice

1) Iteration 1

In the first iteration, the draft ISCP will be reviewed by information security experts and pedagogy / andragogy [9] experts according to certification types, courses, and course content.

A questionnaire will be designed for public enterprises and governmental organization to collect their opinions and revision requests about courses and course content of the Draft ISCP.

Final version of the draft program will be developed by considering the information gathered from information security experts, pedagogy / andragogy [9] experts and people from public enterprises and governmental organizations.

2) Iteration 2

In the second iteration of the certification program data that will be collected by risk analysis and penetration tests will be used for making revisions. The information systems of participant public enterprises and governmental organizations will be tested by penetration test experts and analyzed by risk analysis experts. The findings of these thorough analyses will be used to make minor revisions in the certification program. The identified major system vulnerabilities will provide invaluable information for training requirements.

D. Phase 4: Reflection to produce design principles and enhance solution implementation

1) Development of Courses and Course Content

The content of the courses that are included in the certification program will be developed by subject matter experts. The project manager and the education consultant will prepare a course content template and a guide on how to design courses for the subject matter experts in order to secure standardization of course material. All the course content development will be planned by the project manager and the subject matter experts will be informed of the development process and deadlines with a brief presentation.

The Attacks / Defense Documentation Library prepared in the second project of the program will be the major source of training materials.

2) The Preparation of Certification Exams

Upon the completion of ISCP, the proficiency of the participants will be evaluated by certification exams. The subject matter experts are expected to prepare certification exam questions which will be stored in the certification exam question database. An online exam framework will be used in order to prepare, implement, and evaluate results of certification exams. The online exam framework will be able to provide reports for both participants and the public enterprises.

3) ISCP Pilot Study

The developed ISCP will be implemented as a pilot study with the voluntary public enterprises and governmental organizations in Turkey. The results of the pilot study will be used to make minor corrections and revisions in the proposed certification program.

4) The Implementation and Evaluation of the ISCP

The proposed certification program will be implemented with the participants from public enterprises and governmental organizations and then an evaluation report will be published for both the individual participants and the organizations. The results of the certification exams will be the major determinant for the proficiency of the certification program. After the implementation of the certification program the opinions of the individual participants and the organizations about the program will be asked in order to enhance and revise the certification program before the next implementation.

5) The Overall View of the Proposed Program

The PISSP consists of 3 inter-related projects. These are;

1. Training Project,
2. Documentation Project,
3. Risk Analysis Project.

Although this paper is focuses on the Training Project of the PISSP, the relationships between the projects are important to understand the overall picture. These projects are not independent from but they are inter-related with each other as shown in Figure 3.

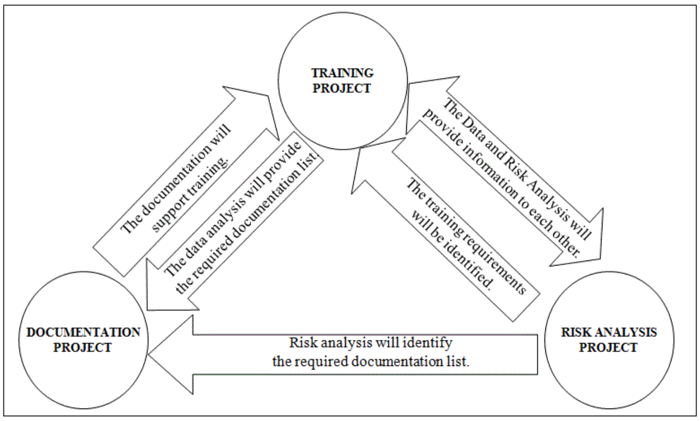
TRAINING PROJECT
The documentation will support training.
The data analysis will provide the required documentation list.
The Data and Risk Analysis will provide information to each other.
The training requirements will be identified.
DOCUMENTATION PROJECT
Risk analysis will identify the required documentation list.
RISK ANALYSIS PROJECT

Figure 3. Relationships between the Projects

In the Training Project, the data analysis phase will provide information on the required documentation list that will be prepared in the Documentation Project. The documentation will be used as training support material in the implementation phase of the Training Project.

On the other hand, there is a two way relationship between Training Project and the Risk Analysis Project. The results of the Risk Analysis project will determine the training requirements of the employees of the organizations based on the system vulnerabilities and employee incompetency. The data analysis in the Training Project and the results of the Risk Analysis Project will provide revision information for the next iteration.

The results of the Risk Analysis Project will determine the major documentation requirements based on the identified system vulnerabilities. The documentation prepared in the Documentation Project will be served online for the Public Enterprises and Governmental Organizations to support their system security implementations.

IV. THE CURRENT STATE OF THE PROPOSED PROGRAM

A. The Draft List of Courses in The Training Program

The analysis conducted in the Phase 1 about the current state of information security in the public environment and the development of draft information security training program in the Phase 2 enabled to develop a complete list of the trainings included in the curriculum. The draft training program list of trainings are given in the Table 1.

No	Course Name
1	User Security Awareness
2	General Security for Managers
3	Social Engineering: Attack and Defense Methods
4	ISO 27001 Implementation and Auditing
5	Business Continuity and Disaster Recovery Planning
6	Windows Security
7	Microsoft Systems Security
8	Computer Security and Incident Response Team Setup and Management
9	Unix / Linux Security
10	Network Forensics
11	File System Forensics
12	Perimeter Protection
13	Wireless Network Security
14	Oracle Database Security
15	Microsoft SQL Server Database Security
16	HTTP Based Application Security
17	Fundamental Security Auditing
18	Common Criteria (TS ISO/IEC 15408)
19	Smart Card Side Channel Analysis and Reverse Engineering
20	Central Security Monitoring Systems

No	Course Name
21	DDoS (Distributed Denial of Service Attack) Prevention
22	Malware Analysis
23	Secure Software Development Life Cycle
24	Secure JAVA / .NET / PHP Application Development
25	Penetration Testing
26	Information Systems Auditing
27	Mobile Device and Communication Security
28	Central Logging and Warning Systems Security

Table 1. The Draft List of Courses

B. Major Adjustments in the Course List

1) Perimeter Protection

A major change acted on “Perimeter Protection” training. This training covers one of the most critical components of enterprise security. After some discussions, it was decided to partition this training course into seven different trainings. Below is the list of trainings which are introduced in place of “Perimeter Protection” course. Such a partition has also facilitated to set some of these newly introduced courses as prerequisites for other courses in the whole training list.

Course Name	Number of Days
Introduction to TCP/IP from Security Perspective	2 days
Security of Active Devices	2 days
Intrusion Detection and Protection Systems	2 days
Firewalls and Virtual Private Networks	2 days
Load Balancers and SSL Off-Loaders and SSL Accelerators	1 day
Network Monitoring Software	1 day
Network Access Control (NAC) and 802.1x	1 day

Table 2. Perimeter Protection Courses

2) Smart Card Side Channel Analysis and Reverse Engineering

This course will be not being delivered to all program participants and therefore will not be in a part of the curriculum. On the other hand, this course will be prepared and delivered as private training if need arises.

3) Common Criteria (TS ISO/IEC 15408)

It was decided that this course will not be beneficial to most of the participants. On the other hand, we are assured that the concept of Common Criteria is to be known at least to management personnel in information systems. Therefore, this course will be a part of the training “General Security for Managers”.

4) Information Systems Auditing

It was also decided that program participants are not in the potential target audience of Information Systems Auditing training course. Therefore, this course will be updated according to newly introduced methodology but kept as private and excluded from the curriculum.

C. The Final List of Courses in The Training Program

The final list of courses in the training program formed after the major adjustments is given in the Table 2.

No	Course Name
1	User Security Awareness
2	General Security for Managers
3	Social Engineering: Attack and Defense Methods
4	ISO 27001 Implementation and Auditing
5	Business Continuity and Disaster Recovery Planning
6	Windows Security
7	Microsoft Systems Security
8	Computer Security and Incident Response Team Setup and Management
9	Unix / Linux Security
10	Network Forensics
11	File System Forensics
12	Perimeter Protection
13	Wireless Network Security
14	Oracle Database Security
15	Microsoft SQL Server Database Security
16	HTTP Based Application Security
17	Fundamental Security Auditing
18	Central Security Monitoring Systems
19	DDoS (Distributed Denial of Service Attack) Prevention
20	Malware Analysis
21	Secure Software Development Life Cycle
22	Secure JAVA / .NET / PHP Application Development
23	Penetration Testing
24	Mobile Device and Communication Security
25	Central Logging and Warning Systems Security

Table 2. The Final List of Courses

The next phase of the training program is to develop the courses in the final list. In order to standardize the development of courses a solid framework is developed.

D. A Solid Framework for Training Preperation and Review Process

In an attempt to provide a solid framework for training developers to ease and standardize training development process, it was decided that training developers are to follow a document so called “Training Preparation Guide for Training Developers” strictly so that the resulting training documents adhere to predetermined standards. "Training Preparation Guide for Training Developers" document includes the following detailed information.

For a better and efficient review process both for the very first release of the training content and the document updates in its life-cycle, training content will be kept as Microsoft Word document. A dedicated Microsoft Word document is stored and maintained along with the training presentation (in form of Microsoft PowerPoint). Any change requests (if decided so) are to be made to this word document and reflected onto the training presentation by the responsible of each training course. This made it possible to track the changes in time and facilitated an approval process.

This word document will mainly address the following list of items.

- Training objectives and expected target audience
- Description of the training environment
  - What kind of a training class is required?
  - Required connectivity preparations before each class
  - Tools or software to be installed on both servers and student computers
- Skeleton of the training
  1. Determine ***tasks*** expected to be achieved by the attendee after a successful class attendance
  2. For each ***task*** determined in item (i), find out the ***skills*** and ***knowledge*** required in order to fulfill that ***task***
  3. For each **skill** or **knowledge**, state whether an activity or demo should be prepared
  4. Not all the **skills** or **knowledge** is eligible to be included in the training content. It is to keep all the determined **skills** and **knowledge** requirements in this word document but not all of them are to be reflected onto the training content.
- Training Content
  - The skills and knowledge which are determined in Section "Skeleton of the training" and decided to be included in training content have to be grouped into logical classifications so called modules. Modules represent the different chapters of the training course. The skills or knowledge required to achieve different tasks may fall into the same module. So tasks determined in Section "Skeleton of the training" do not play an integral role while putting skills and knowledge into modules.
  - A group of knowledge and associated skills comprise a slide or a logical slide with multiple physical slides. Such a logical slide is to be represented as a heading in the training word document. This is required to map PowerPoint slides to word document and apply comments or change requests on the word document.
- Training Content Design

Under this heading, the approach of content preparation is given. Training developers are instructed to put students into the center of the materials and class. Developers are also encouraged to prepare materials so that they don't teach but let the attendees learn themselves on hand of activities, exercises or samples. This heading also covers the handling of other resources if directly or indirectly used.

- Training course summary to be used in the training catalog

Training developers are advised to create a summary of the training to address;

  - The target audience
  - Main tasks identified
  - Training format (type and level of activities)
  - Presumable prerequisites
  - Main modules identified.
- Preparation of the PowerPoint presentation

A template PowerPoint document is provided to the training developers so that look and feel will be the same for all the trainings. Addressed topics are as follows;

  - Font type and minimum font size
  - A slide will be reserved to show the upcoming module and slide notes section will include a paragraph to summarize the content.
  - The content directly used from another resource is to be displayed with its reference.
  - Slide notes will explain the slide content in detail.
  - A guide PowerPoint is also provided to address the usage of fonts, effect of colors and space for the human beings.
- Technical Review of Training Materials

A pilot run will be accomplished. This pilot class will include one or two technical experts as well as some personnel from information systems security field. The comments of the attendees will be discussed after the training and will be reflected onto the training materials if accepted.

- Update Process for Training Materials

In the life-cycle of training materials, it is critical that not the PowerPoint but the word document is accepted as the main training course material. Change requests coming from the attendees or arisen somehow are to be submitted to the training owner. Training owner will communicate with the expert in field to approve the change and starting from the word document, reflect the changes on the training materials. PowerPoint slides are numbered in order to ease the process of locating the changes.

V. Conclusions And Future Plans

The designed Information Systems Security Program is still at the initial phases of development and the analysis work is in progress. The developmental approach of the program promises important opportunities for and contributions to future work.

The use of design-based research will provides the following advantages;

- designing the program in collaboration with researchers, program target groups, information security experts and education experts,
- integrating design principles to find solutions of complex learning objectives,
- testing and revising the proposed program by the iterative process approach.

The design-based research approach to develop an Information Systems Security Program will provide an appropriate and useful means of designing a practical training program in the context of the learning environment itself. As Van den Akker [10] defines, the purpose of a design-based research activity is to reduce, 'uncertainty in decision making in designing and developing educational interventions'. Similarly, design-based research is a type of risk management that enables the researcher to control the risks in the design of an educational program. In this respect, the outcome of the research will be applicable in practice. This is ensured by developing a solution, then testing and revising the solution in practice, which will result in the final program.

The PISSP will be implemented in 3 years' time for all the public enterprises and governmental organizations in Turkey. The program is funded by the Turkish Ministry of Development. The major aim of the program is to increase the information systems security level of public enterprises and governmental organizations in Turkey.

With the Training Project the employees of public enterprises and governmental organizations will be trained on system security concepts. The Documentation project will provide necessary systems security guidelines on how to secure the information assets of public enterprises and governmental organizations. The Risk Analysis project will secure the information systems of public enterprises and governmental organizations by penetration testing and then taking preventive measures for the determined vulnerabilities.

It is clear that information security education is a need and there are many studies [11] [12] [13] demonstrating or focusing on the importance of information security education. For public enterprises and governmental organizations it is a vital need since their information assets are critical for the whole country. The PISSP is a work in progress and the results of the program will provide valuable information about the current information security status in Turkey, and more secure information systems infrastructure in the public enterprises and governmental organizations.

Acknowledgment

Ünal Tatar and Bilge Karabacak contributed to the design of the PISSP.

References

[1] Amiel, T., & Reeves, T. C. (2008). Design-Based Research and Educational Technology: Rethinking Technology and the Research Agenda. Educational Technology & Society, 11 (4), 29–40.

[2] Stanton, J.M., Caldera, C., Isaac, A., Stam, K.R. & Marcinkowski, S.J. (2003). Behavioral IS security: Defining the criterion space. In: Mastrangelo P.M. & Everton W.J. (eds). The Internet at work or not: Preventing computer deviance. Symposium presentation at the meeting of the society for Industrial and Organizational Psychology, Orlando.

[3] Delp, B.T., Nuristani, S., and Mitchell, B. Cybersecurity: Congressional Actin, Public-Private Partnership, and Education are Key to Mitigating Vulnerabilities, The CIP Report, 9 (7), January 2011.

[4] Parker, D.B. (1998). Fighting Computer Crime: A new Framework for Protecting Information. John Wiley & Sons, USA.

[5] Siponen, M.T. (2000). A conceptual foundation for organizational IS security awareness. Information Management & Computer Security 8(1): 31-41.

[6] Aytes, K. & Connolly, T. (2003). A research Model for Investigating Human Behavior Related to Computer Security. Proceedings of the Ninth Americas Conference on Information Systems: 2027-2031.

[7] Wang, F. and Hannafin, M.J. (2005). Design-based research and technology-enhanced learning environments. Educational Technology Research and Development, 53(4), 5-23.

[8] BTK and TÜBİTAK (2011). "The National Cyber Security Exercise Final Report 2011" WWW Document viewed 20/02/2012 from http://www.bilgiguvenligi.gov.tr/dokuman-yukle/raporlar/usgt-2011-en/download.html

[9] Knowles, M. (1987). Adult learning. In R.Craig (Ed.), Training and development handbook (pp. 168–179). New York: McGraw-Hill.

[10] Van den Akker, J. (1999). Principles and methods of development research. In J.van den Akker, N. Nieveen, R.M. Branch, K.L. Gustafson, & T. Plomp, (Eds.), Design methodology and developmental research in education and training (pp. 1-14). The Netherlands: Kluwer Academic Publishers.

[11] Perez, T.J. (2011). Information Security Education: A Competency Based Approach and Exemplification. Proceedings of the 15th Colloquium for Information Systems Security Education Fairborn, Ohio June 13-15, 2011.

[12] Cooper, S., Nickell, C., Pérez, L. C., Oldfield, B., Brynielsson, J., Gökce, A. G., Hawthorne, E. K., Klee, K. J., Lawrence, A., and Wetzel, S., Towards information assurance (IA) curricular guidelines. In Proceedings of the 2010 ITiCSE working group reports on Working group reports (ITiCSE-WGR '10), Alison Clear and Lori Russell Dag (Eds.). ACM, New York, NY, USA, 49-64.

[13] Crowley, E. Information System Security Curricula Development, 2003, ACM.