Association for Information Systems
AIS Electronic Library (AISeL)

MCIS 2009 Proceedings

Mediterranean Conference on Information Systems (MCIS)

2009

Integrating Disaster Recovery Plan Activities Into The System Development Life Cycle

George Aggelinos
University of Piraeus, Dept. of Digital Systems, gaggelinos@yahoo.com

Sokratis Katsikas
University of Piraeus, Dept. of Digital Systems, ska@unipi.gr

IS SECURITY AND PRIVACY

INTEGRATING DISASTER RECOVERY PLAN ACTIVITIES INTO THE SYSTEM DEVELOPMENT LIFE CYCLE

Aggelinos, George, University of Piraeus, Dept. of Digital Systems, 150 Androutsou St., Piraeus GR-18532, Greece, gaggelinos@yahoo.com
Katsikas, Sokratis, University of Piraeus, Dept. of Digital Systems, 150 Androutsou St., Piraeus GR-18532, Greece, ska@unipi.gr

Abstract

The development of an IS for an organization is a project of a strategic nature. The development process is a time-consuming and special budgeted project that follows the six stages of the System Development Life Cycle (SDLC). Integrating security within the SDLC is a very important issue. The security of an IS is designed at the very early stages of its development. A security object that is nowadays a must is the Disaster Recovery Plan. Security questions like "Is the Information System Security an issue that has to be a matter of concern for the organization from the start of Information System development?" and "At which stage of its development does an Information System begin to be at risk ?" concern both the organizations and the developers. This paper proposes the enhancement of the SDLC stages in order to reduce the risks from the start of a development, by integrating the development of the Disaster Recovery Plan into the SDLC process. Details are given on how to achieve this, as well as the reasons and the benefits to the organization and to the manufacturer.

Keywords: *Disaster Recovery, SDLC, Information System Development, Information System Security, Data Security*

1 INTRODUCTION

In the early days of IS, decision making – at all levels of an organization – was made based on manually processed information. This information was the result of a time-consuming gathering effort in a market that did not change so fast. Moreover, the competition was "local" or "regional" and only occasionally "national" or "international".

As the nature of the competition started to change and became more global, the need for accurate, timely and effective decisions increased. These decisions, most of the times, reflect the organization's reactions to the market in order to avoid or overcome the competition. These reactions are strongly dependent on the information that the organization perceives about the market or even about its administrative operations, as, in the era of the Globalization, the competition may come by an unknown and invisible competitor who can operate better. Thus, reactions will have to be more sophisticated, which means that organizations cannot afford to rely on decision-making without the support of some Information System, the utilization of which seems to be indispensable nowadays.

The increasing adoption of IS by organizations in all industries has led them to install ISs which, most of the times, are "suited" to their needs rather than "tailored" to those. This happens because the majority of the organizations face the IS as a cost center (Souliotis & Papadakis 2007); hence they try to reduce its installation expenses at the expense of compromising their needs. By operating this compromised system, organizations depend themselves more and more upon it; thereupon, they cannot operate without being supported by the IS.

On the other hand, the development of an IS tailored to the needs and requirements of an organization is a very serious project. Usually organizations face the administration of such a project as a technical project. The organization appoints someone with technical responsibilities in charge of the IS development, expecting that s/he will be able to understand and satisfy the functional-business requirements of the organization. When this is the case, the development of the system is more "technically oriented" than "business" or "function oriented". The person charged with the administration of the project has to control financial, functional, administrative (e.g. approvals) and social activities (like resistance to change) in order for the investment not to fail. The development and installation of an IS for an organization is an effort proportional to the magnitude of the organization. Thus, the failure of an IS development project may bring the organization to a financial crisis (Stefanou 2003). Instead, the success of the project can give the organization the competitive advantage (if the system is innovative), better administrative self-control or it may help bring into effect a strategic target. For these reasons, organizations have to appoint a top executive for leading the IS development project, who will also have decision making rights. The most important reason for charging a top executive with the leadership is that s/he has to make decisions about the development of the system, which will affect the organization in its business nature. A number of such decisions pertain to the security of the Information System.

A survey (Rainer et al. 2007) about the way that Business Managers and Information Security Professionals view information security issues reveals that the two groups have different views on security. However, it is interesting to note that the "*Business continuity and Disaster preparation*" issue is listed among the top-10 of 142 security items (managerial and technical), a fact indicating convergence in the views of both groups. The IT Disaster Recovery Plan (DRP) is significant to the organization, due to the dependence of the organization on the IS. Depending on the business sector that the organization is active in, its survival may be directly linked to the operation of its IT system. We can take as an example the case of a bank, or a financial organization or a healthcare establishment (HCE). A possible disaster of its IS forces the organization to interrupt its operations until the system is rebuilt to a point of being capable of servicing at least the organization's basic needs. In view of the consequences of being out-of-business for prolonged periods of time, the decision for the development of an IT-DRP for the security of the IS seems to be unavoidable for such organizations. The process for developing an IT-DRP is very demanding and one through which the organization learns itself better, in order to decide about the level of the disaster protection that it wants to apply. At the beginning of the DRP development a Business Impact Analysis (BIA) will identify and categorise the Critical Business Functions (CBFs) that are necessary for the organization's survival. The results of the BIA will be the basis for the Risk Analysis tailored to the needs of the specific IS (Aggelinos & Katsikas 2007). At this point the organization is able to define its recovery strategy and then to proceed with formulating its IT-DRP, taking into account at least the off-site storage, the place and kind of the recovery site. It is also able to establish its Recovery Time Objects (RTOs) and Recovery Point Objects (RPOs). The Disaster Recovery Plan has to be directly linked to the Business Continuity Plan (BCP), so as to support the business functions that the organization wants to recover immediately, i.e. the CBFs.

Accepting the view that the development of an Information System is both a technical and a business issue, the organization has to reconsider its attitude about IS development. As the IS can affect the whole organization positively or negatively, the development of an IS has to be considered as a strategy and not as a cost center (Souliotis & Papadakis 2007). As a strategy target, the IS has to be protected against the risks that may threaten it. Here, a very important question arises: "*Is the Information System Security an issue that has to be a matter of concern for the organization from the start of Information System development process?"* The answer to this question cannot be given readily but it generates another one important question: "*At which stage of its development does an Information System begin to be at risk?*"

This paper attempts to answer these two questions while indicating to organizations the way to act in order to have a secure development which, in turn, leads to protecting their investment. It proposes

enhancing the System Development Life Cycle (SDLC) stages with Disaster Recovery Planning (DRP) activities, in order for the system to be ready for emergency operation at the end of the implementation stage.

The remaining of the paper is structured as follows: In Section 2 we review the standard system development life cycle. In Section 3 we propose enhancing the standard life cycle model with DRP-related activities; in Section 4 we examine the benefits from adopting such an enhancement and we conclude with Section 5.

2 SYSTEM DEVELOPMENT LIFE CYCLE

The development of an Information System either suited or tailored follows a general procedure known as System Development Life Cycle (SDLC). This cycle follows six (6) stages, which are shown in figure 1 (Weaver et al. 2002). In the case of a suited IS, some initial activities have already been performed by the manufacturer, but in the case of a tailored system these activities have to be performed by the organization. In both the "suited" and the "tailored" case, the SDLC starts with the "Strategy Planning" stage, a fact denoting that any decision about the development of a system has to have a strategic orientation to serve a strategic target.

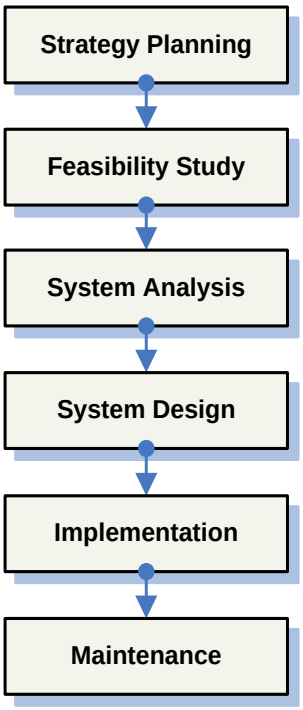

Figure 1: Traditional System Development Life Cycle (SDLC)

When developing an IS, an organization runs an IS development method and covers the first four stages of the SDLC. The structure of many IS development methodologies follows that of the SDLC. Of these methodologies, perhaps the most well-known is the Structured Systems Analysis and Design Methodology (SSADM). It is the standard information systems development method for UK government projects, and has become a *de facto* standard for the UK private sector (Weaver et al. 2002), (Down et al. 1992). The Implementation stage of the SDLC includes the trial period and the final acceptance of the information system by the project administrator. In the trial period, the system is operated by the users in their daily duties in order to ascertain the problems and resolve them. After that, the system is fully operative and it must be protected against security risks.

Deploying security measures and educating users accordingly is a time-consuming process, whose time requirements depend on the size of the system, as the time needed for training the users on a system with standard objects (e.g. strange emails, deceptive web sites, frequent password changes etc) is quite reduced compared to that needed for another system that uses more complex measures, such as cryptographic keys, USB identifiers, smart cards etc. If all this is done after the system has been put into productive operation, the resulting time-gap during which the system is unprotected (or at least under-protected) may become very important, particularly if the information system replaces a legacy system, as is more often than not the case nowadays. A possible disaster (physical or logical) at this point could bring the organization to a very difficult financial and legal position. The organization will not be able to fulfil its obligations, and the time to recover and to come back to "business as usual" can prove crucial for its future. In addition, the organization will have spent a vast amount for an IS that will not be able to use even in its simplest operation. At this point, the organization will realize that it should have been protected against a potential disaster and that it should have provided for emergency operation of the system. Given the limited resources that may be allocated for emergency operations, the organization should have pre-decided the business functions that could be served in case of emergency and, consequently, the logical and physical design of the pertinent requirements.

Therefore, an Information System begins to be at risk early in the SDLC, when entering the implementation stage, at the end of which the IS is at full risk. The extent of the risk that an organization takes cannot be unambiguous because the value of the system for the organization is subjective and depends on the value that the IS perceives by the information it processes [*quantitatively* (financial use) or *qualitatively* (decision making use)]; the degree to which the organization relies upon the system; the budget of the investment; the extent to which the system is used within the organization; the capability of the organization to switch swiftly to a manual mode of business operations; and a number of other, less significant, factors. The mitigation of this risk has to be proactive rather than reactive. For this reason, the security design of the system has to focus on approaches that ensure effective counteraction on potentially problematic areas (Tryfonas & Kiountouzis 2001). This in turn means that the organization has to be ready for Emergency Operation (EO) at the end of the implementation stage. The EO is completely different than the Normal Operation (NO), and requires different and fast deployment of pre-decided plans.

The fact that information security designs should be carried out as early as possible in the system development lifecycle and particularly should be incorporated within the system requirements specification stage has been long established (Baskerville 1993, Kalloniatis et al 2008). It has also found its way into relevant standards (Kissel et al. 2008), where it is recommended that many security issues are dealt with in the initiation phase of a 5-phase SDLC– which corresponds to the Strategy and Feasibility Study stages. However, it is unfortunate that this long established and well known -among information professionals- has still a long way to go to be observed in practice. A doctoral thesis (Tryfonas 2003) has studied the difficulties of integrating security into the traditional system development life cycle and has reached the conclusion that the security analysis of a system in the form of specifications/provisions is performed *only after the end* of its development. The same holds true even more for DRP development activities. Taking into account the fact that the development of a DRP may take anything from some weeks to two years –depending on the size of the organization and of the system-, it seems, by direct analogy reasoning, that by enhancing the traditional SDLC stages to include DRP development activities in early stages of the process one would avoid having a system at risk for long periods of time.

3 ENHANCING THE SDLC STAGES

In view of the above, it seems that the earlier the DRP is completed, the better to the IS development stakeholders. Therefore, we propose enhancing the SDLC stages in a way so that the Disaster Recovery Plan will be ready at the end of the Implementation stage. Figure 2 depicts the proposed enhancements.

As it can be seen, the enhancement of the stages is done in a hybrid manner, taking into account the hierarchical structure of the SDLC model. In the first four stages, DRP activities run in parallel with the activities concerning the development of the system in normal operation. This means that the normal operation development can move to the next stage in order to save time, but the completion of the stage will be done only after taking into account the DRP decisions/activities for emergency operations. In the two last stages the DRP activities are appended to those of normal operations development. This means that the stages cannot be completed – and consequently we cannot move to the next stage – without having completed the corresponding DRP activities. In each stage of the SDLC a deliverable has to be produced, which will provide the basis for the next stage, thus requiring an extensive documentation to be produced within each phase (Stefanou 2003).

In more detail, in the *Strategy Planning* stage the organization may decide about the target of the development, the deadline, the project manager, the business units that will be served, the amount to spend, outsourcing, the developer, the conformity with laws and standards, the level of maintenance (SLAs), third parties connection capability and a number of other decisions for normal operations. These decisions are enough to move to the next stage – always concerning normal operations.

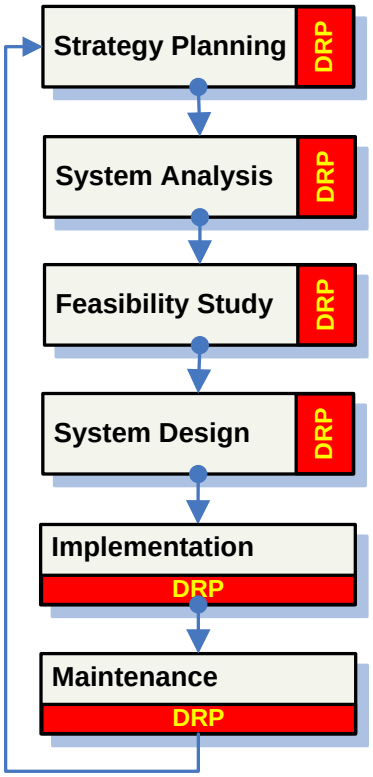

Figure 2: Altered System Development Life Cycle (SDLC)

In the DRP parallel section, the strategy planning of the organization, has to include decisions about emergency operations that will allow the proper design of the EO system. These decisions pertain to the site and the precise location where the system will operate in EO; the kind of site (cold, hot, warm); the business units that need to be covered; the desired switching time to EO; initial RTOs and RPOs (e.g. equipment procurement in the first 6 working hours); the maximum time allowed to remain in EO; the incorporation of the plan into the annual budget; the percentage of the NO system budget to be spent for the EO system; the DRP coordinator; the alliances with similar organizations for mutual assistance; the standards for conformity (e.g. BS-7799, ISO 27001, BS-25999); and some more DRP strategy

planning decisions such as revision time, liabilities and responsibilities at managerial level etc. (Aggelinos & Katsikas 2007).

In the *Feasibility Study* stage the organization has to consider the technical, financial, legal, operational, organizational and the strategic feasibility of the development and (or) the acquisition of the system. There is a practical difficulty here: The Feasibility Study needs as input information that is produced in the next stage, as it is impossible to have accurate information about the requirements that need to be covered and about the risks with their proposed solutions. Without this information, the results of the study will be either overestimated or underestimated. In either case the project is jeopardized due to improper budgeting. This is why we adopt the usual analyst's practice, according to which the Feasibility Study is performed after the System Analysis stage, when the organization knows exactly what it wants to do and what it has to pay for. This practice is more expensive for the organization but it is safer for the execution of the project and the whole investment.

In the next stage, the *System Analysis*, the organization first has to investigate the existing system (if any) and generally the informational environment that already exists. This organizational study has to be documented, taking into account all the electronic and hard copies, the user information needs, data flows etc. Then the stage proceeds with the analysis of the documented investigation findings. The deliverable of this stage is a report including the current situation (such as the kind of data, data flows, available systems and their users, user problems, hardcopy templates, etc) and the situation that needs to be served (such as new business units, user requirements, new data flows, user rights, electronic required approvals, external/third party connections, initial security policy requirements, conformity with law and regulations etc).

In the DRP section of the stage, the organization investigates its functions performing a BIA in order to identify and categorise the CBFs that are necessary for its survival. In this procedure the organization has to (Aggelinos & Katsikas 2007) list the business functions and categorise them in order of importance; link business functions to applications and systems; identify the functions that affect the existence of the organization; assign RTOs and define RPOs for each business function; assign recovery priorities according to organizational and technical criteria; define the term of the disaster for the organization and the criteria for the activation of the plan according to the CBFs; consider its legal responsibilities from the possible disaster; and estimate the potential loss revenue for every day remaining "out of business" in order to have a possible trade off for extra emergency expenses. In order to perform a meaningful BIA in this early stage of the development process, we consider the business functions according to their significance regardless of the technology used to implement them (manually or IS based). CBFs are categorised considering how they are supported by the Information System.

The BIA will be completed after the decisions on the above issues are approved. These will form the basis for the Risk Analysis of the IS. The Risk Assessment procedure has to assess the risks for the CBFs only and not for all the functions, thus saving enough time and resources. The assessment will include at a minimum (Aggelinos & Katsikas 2007) the general risks and their occurrence probability; the list of the risks for any CBF and system; the link of the occurrence probability of any risk to every function or system in order to find how probable it is for a system to be affected; the proposed solutions for every combination: Risk-CBF or Risk-System. Dealing with a risk is directly connected to a cost-benefit analysis in order to remain profitable for the organization (Baskerville 1993); define the security categorization of the system(s) according to an appropriate standard such as, for medical information systems the CEN ENV 12924 (CEN 1997); and define the disaster recovery policy of the plan according to the general security policy. The completion of the RA will give the results as a basis for the next stage, the Feasibility Study.

Here is the adopted position where the *Feasibility Study* can take place. The deliverable of this stage is a report specifying – at least – the technical and business basis, the objects of the project, the associated risks, the alternative solutions and finally the cost/benefits analysis. The above requirements take their

information from the BIA, RA and the general report of the System Analysis. In the DRP parallel section of the stage the organization has to investigate if the decisions for the EO system can be covered by the budget (e.g. off site storage, kind of site, equipment, etc); the exact costs and benefits for the organization from the development of such a plan; the real amount that needs to be budgeted for EO according to the BIA, the RA and the proposed solutions (e.g. the total amount for recovery in 3 days is 100,000€ while for recovery in 10 days is 68,000€); and the changes that will be brought to the organization from the development of the DRP (e.g. DRP coordinator position, testing of recovery capabilities every year, predicting the annual budget for recovery purposes, etc). The results of the study have to be documented in a report to the top management.

The next stage, *System Design*, is the most important stage of the SDLC because it gives the solution to the problems and requirements. The design consists of the logical and physical design taking into account also the human resources and the procedures established in the organization. Here is a basic problem: *the suited system changes the procedures of the organization* (resistance to change due to inconvenience) in contrast with the tailored system, which transforms manual procedures into electronic ones (more expensive). The deliverable is a report containing all the specifications for the construction of the new system. The importance of the stage is due to the fact that any fault or bigger tolerance to problems may lead to insuperable obstacles which are translated to administrative inconveniences or to big amounts of money necessary to fix the problem. Either case may lead to a strong resistance to change, practical non-acceptance of the system and consequently general failure of the project, resulting in a significant impact on the general strategy of the organization to realize its targets.

The DRP section of the stage examines the operations/functions that have to be covered in EO, i.e. the CBFs and some supportive functions. These are the business units; the procedures that will be supported in each business unit; the operating applications; the necessary physical equipment to cover the needs (e.g. two servers instead of five); the number of users that will be supported by business unit; the connections of remote users or third parties; the required related security of the system (e.g. persons that have physical access); special requirements only for EO (e.g. number of users connected to an application at the same time, restrictions of printing etc); and practical tests according to a methodology based on: 1) scenario, 2) trigger events, 3) a function, 4) a system (Aggelinos & Katsikas 2007).

After this, a corresponding report containing the specifications necessary to operate the system in EO must be filed. This report will have as a basis the report that was produced for NO; this means that any change or alteration to the Normal Operations report may lead to changes or alterations to the Emergency Operations report. At this point, the parallel character of the SDLC enhancement ends and the hierarchical character starts.

In the *Implementation* stage the software will be developed or adapted and the hardware will be acquired to serve the software, both according to the specifications of the previous stage. The test & documentation phases will have to be completed before the delivery of the system to the users for a trial use. Any alterations coming from the trial phase have to be documented and the system is ready for use. This stage has not finished yet.

In the DRP section the activities are strictly related to the kind of the site (cold, hot, warm) that has been decided in the Strategy Planning stage. According to the kind of site the organization may have to activate EO contracts or mutual agreements; rent a place for some days; buy or rent some equipment for some days in order to execute tests; set up the EO system to work without users; count the real RTOs and switching time; load the system with the predefined users; operate for some hours (if possible); organize the off-site storage of the plan and its objects (e.g. data & application backups); assess the procedures, designs, duties, responsibilities etc of the documented EO plan during a test; define the time of reviewing the plan (e.g. anytime: alterations, semi-annually: check the corrections of the alterations, annually: review the whole plan); educate a recovery team on the recovery procedures

(e.g. in the knowledge of: the procedures' specifications, their duties in the team etc [classroom education]); and certify the whole system according to the standard decided in the Strategy Planning stage.

The weaknesses observed during this execution have to be fixed, so as the Emergency Operations system fulfils the requirements that have been decided for EO. After that, the Disaster Recovery Plan has to be documented as a technical plan and it also has to include the procedures needed for its implementation (e.g. who has to order the purchase of the equipment, its reception, the place to receive it, the maximum time after the order etc). At the end of this stage, when the plan is not tested yet, the legacy system should remain intact and operational as a contingency to the replaced information system until, at least, the new system has been sufficiently tested (Swanson et al 202).The Implementation stage is completed at the end of the DRP documentation phase.

With the last stage *Maintenance*, the System Life Cycle begins. This is the largest stage where the system is fully operational and the organization makes the depreciation of the investment. During this stage the organization may have some new requirements to fulfil or have to change/alter some existing ones due to the changing environment (e.g. laws, new business units). Any change or alteration has to be documented for the normal operations system. As for the DRP section, a decision has to be made, on "*Is this change/alteration an issue for the emergency operations system?*" – changing, also, the DRP documentation in the case of a positive answer. The specifications in hardware & software, the produced data and their backup, the users etc have to be documented for implementation in EO immediately after the end of the change/alteration, in a standard and controlled manner (Configuration Management) (Ross et al 2009). If there are many or very important changes to be made on the IS, then the Strategy Planning stage has to be executed again and a new smaller development cycle is starting. The reviews of the whole Disaster Recovery Plan have to be performed in the predefined time aiming the synchronization of the plan. The practical testing of the plan can take place in an empty room or in the (contracted) cold site in order to check gaps in the plan, RTOs, RPOs etc. The duration and the extent of the test depends on the obtainable budget and the importance that the management gives to the recovery.

A practical issue that has to be made clear is that only one report deliverable is the outcome of any stage. The report has two sections: the first for Normal and the second for Emergency Operations.

Table 1 summarizes the SDLC stages for N.O. system development and DRP activities and Deliverables.

SDLC stages	Normal Operations Activities & Deliverables		DRP Activities & Deliverables		
Strategy Planning	*Stage activities for Normal Operations System development*	*X*	Site & Location	X	
			Kind of site	X	
			Business unit to be covered	X	
			Switching time to E.O.	X	
			Initial RTOs & RPOs	X	
			Maximum time in E.O.	X	
			Incorporation in the annual budget	X	
			Percentage of N.O. budget to E.O. budget	X	
			DRP coordinator	X	
			DRP alliances	X	
			Conformity standards	X	
			Revision time	X	
			Liabilities & responsibilities	X	
			Documented report		X
System Analysis	*-//-*	*X*	BIA	X	
			RA	X	

			Disaster Recovery Policy	X	
			Documentation of report		X
Feasibility Study	-//-	*X*	Investigation for the covering of the DRP needs according to budget	X	
			Real amount according to BIA & RA	X	
			Changes to the organization	X	
			Cost & benefits	X	
			Documented report		X
System Design	-//-	*X*	Analysis of the functions for covering in E.O.	X	
			Business unit: procedures, users, remote connections	X	
			Special requirements	X	
			Practical tests	X	
			Documented report		X
Implementation	*Stage activities for Normal Operations System development with deliverables*				
	DRP activities according to the kind of site			X	
	Documented report				X
Maintenance	*Stage activities for Normal Operations System development with deliverables*				
	Is this change/alteration an issue for the emergency operations system?			X	
	Documented report				X

Table 1. *In the first four stages the DRP activities can work in parallel with the activities for the development of the N.O. system. In the last two stages the DRP activities start when the deliverables of the stage for N.O. system have been completed.*

4 PRACTICAL BENEFITS

A proposal for modifying a methodology that has been set up and has functioned well for many years may only be seriously considered when there are new significant needs to accommodate that are not covered by the traditional methodology and when the stakeholders of the methodology benefit from the modification. In the general case the stakeholders are the organization that the IS is being developed for and the system developer.

The organization benefits from addressing DRP issues during the SDLC stages rather than after them because:

- It *saves time*, as the DRP can be completed a little after the completion of the implementation stage for normal operation, thus reducing the time during which the organization is unable to handle a disaster. The saved project time depends on the size and the extent of the IS.
- It *reduces the risks to the minimum* in their origin as, having secured the CBFs, the risks that have a significant impact on the organization's ability to fulfil its obligations and purposes are reduced.
- It can *save human recourses*, because all this time it will have assigned project responsibilities to a team for the development of the system. That team may have several full-time members that could work on the legacy system to resolve routine problems/failures.
- It can *learn the system* at its basic needs, taking the experience close to the designers/technicians of the manufacturer.

The above may be translated to monetary terms and be measured in order to give to the organization an absolute monetary value of the DRP implementation during the SDLC.

On the other hand, the system developer is capable of handling the DRP design difficulties in the earlier stages of the normal operations design. When a need for a DRP deliverable is known, a different software design or arrangement can take place for the normal operations in order to serve the DRP needs. As an example, recall that a hospital in emergency operation does not need all the X-ray images

in its database; it only needs those of the in-patients. This need can be easily handled in the database with just a flag triggered by the entry and the exit date and can be provided for in the backup and restore procedures, either for a suited or a tailored system. If this provision has not been taken, the restore procedure may take several hours, thus greatly increasing the RTOs. This kind of treatment makes the DRP deliverable tailored to the special needs of an organization and increases the reputation of the developer as a specialist. Moreover, the developer can achieve earlier project completion when a requirement of the organization is a "DRP deliverable" – which tends to be a standard requirement in the IS development nowadays. Starting the DRP project after the total completion of the normal operations system is equivalent to the design of a system fitted to the special needs of an organization. This period may be significant, depending on the organization and its emergency operation needs making a significant time difference between the traditional SDLC and the proposed one. Additionally, the developer can save human resources by allocating the designer/technician team to another project in the time corresponding to the DRP deliverable. This option reduces the developer's operational costs, thus enabling him to make better offers and to be more competitive with the same number of personnel. This cost reduction can be estimated more accurately if the complexity and the resources needed for the development of the system are known.

Figure 3 depicts the expected development time with and without the DRP-enhanced SDLC. It is evident that breaking up the DRP activities and classifying them in the SDLC stages does not significantly affect the total SDLC time.

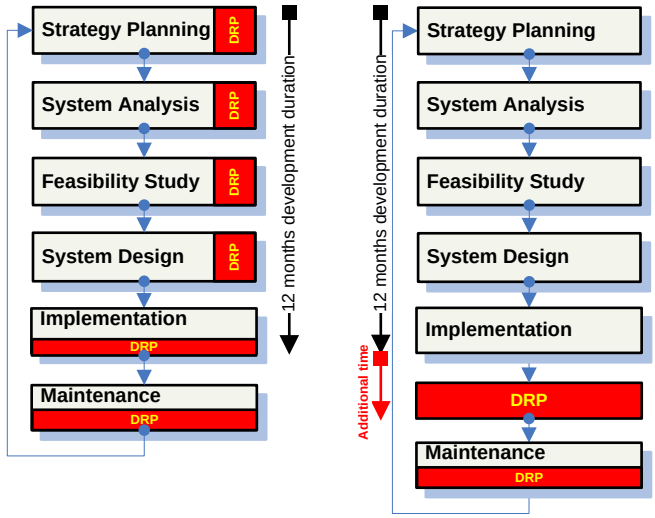

Figure 3: Development time with and without altered SDLC.

5 CONCLUSIONS

The development of an IS for an organization is a very time-consuming, specially budgeted project, the failure of which can threaten the existence of the organization itself. Also, its importance to the administrative function of the organization and to the fulfilment of its strategic and departmental targets is beyond any discussion. Thus, the continuity of operations of the organization is based upon the system to a large extent as the absence of the system makes the organization unable to fulfil its administrative functions and consequently its obligations. By applying the proposed enhanced SDLC, both the organization and the developer can save money by reducing the total time of the project, while at the same time securing the operation of the CBFs by designing a system for EO.

The DRP development will be done taking into account experience and covering emergency operations' needs in the design of the normal operations. This is a procedure that can be carried out without the

pressure of a disaster. Also, cheaper or more adequate solutions can be forecasted in contrast with the solutions obtained under the pressure of a disaster or of a 7/24 operated system.

Last, in the case of a system developed as part of strategic decisions, the existence of the system has to be secured from its initial stages and to be continually secured after the end of its implementation in order to ensure the fulfilment of the strategic goals of the organization.

The enhancement of the SDLC creates the need for another investigation, concerning the incorporation of the DRP objects into the development methodologies that cover the whole system (h/w & s/w), like SSADM or ISAC, and the difficulties that the developers meet using these methodologies. These difficulties derive from the fact that an IT-DRP development is an SDLC for EO corresponding to an SDLC for NO. This investigation is a subject of future research.

References

Aggelinos G., Katsikas S. (2007). Enterprise Recovery in Health Care. In proceedings of the 12th International Symposium on Health Information Management Research – ISHIMR.

Baskerville R. (1993). Information Systems Security Design Methods: Implications for Information Systems Development. ACM Computing Surveys, 25(4).

CEN ENV 12924 (1997). Medical Informatics – Security Categorisation and Protection for Healthcare Information Systems. CEN, European Committee for Standardisation.

Down E., Clare P., Coe I.. (1992). Structured Systems Analysis and Design Method: Application and Context. Prentice Hall (UK).

Kalloniatis C., Kavakli E., Gritzalis S. (2008). Addressing Privacy Requirements in System Design: The PriS Methodology. Requirements Engineering, Vol. 13, No. 3, pp. 241-255. Springer.

Kissel R., Stine K., Scholl M., Rossman H., Fahlsing J., Gulick J. (2008). Security Considerations in the System Development Life Cycle. NIST, Computer Security Division, Information Technology Laboratory. Special Publication 800-64 Rev2.

Rainer K., Marshall T., Knapp K., Montgomery G. (2007). Do Information Security Professionals and Business Managers View Information Security Issues Differently? Information Systems Security, 16, 100-108.

Ross R., Katzke S., Johnson A., Swanson M., Stoneburner G., Rogers G. (2009). Recommended Security Controls for Federal Information Systems. NIST, Computer Security Division, Information Technology Laboratory. Special Publication 800-53 Rev 3.

Souliotis K., Papadakis M. (2007). Politics and economics of health. Papazisis. (In Greek).

Stefanou K. (2003). System Development Life Cycle. Encyclopaedia of Information Systems.

Swanson M., Wohl A., Pope L., Grance T., Hash J., Thomas R. (2002). Contingency Planning Guide for Information Technology Systems. NIST, Computer Security Division, Information Technology Laboratory. Special Publication 800-34.

Tryfonas T. (2003). The Contribution of Organisational Images of Information System Security to the Implementation of Secure Information Systems. Athens University of Economics and Business.

Tryfonas T., Kiountouzis E. (2001). Security Concerns for Contemporary Development Practices: A Case Study. In proceedings of the IFIP TC11, 193.

Weaver P., Lambrou N., Walkley M. (2002). Practical Business Systems Development Using SSADM: A complete tutorial guide. 3rd Edition. Prentice Hall.