INTRODUCTION

1.1 Background

PLN (*Perusahaan Listrik Negara*), established in 1972, is a national company that monopolize the business of electricity supplying in Indonesia. The Pusdiklat (*Pusat Pendidikan dan Latihan*) itself is an unit specialized to conduct educational program and training for whole PLN employee. There are also other main programs offered such as non technical competency certification, assessment of core and role competency, etc.

PLN Pusdiklat have 10 branches called Udiklat (*Unit Pendidikan dan Latihan*), spreading across Indonesia. Having those branches, Pusdiklat act as the central of the information system that supports daily operation. There are some current systems that handled by Pusdiklat which is also involving other branches such as Simdiklat (*Sistem Pendidikan dan Latihan*), file sharing using VSFTP, mail exchanger, e-learning system, e-magazine system, and e-certification system. All those systems are centralized resulting the physical servers itself also located in PLN Pusdiklat.

As growth of PLN is increasing, the need of educational and training program for its employee is also increasing. As a result the information system data in PLN Pusdiklat also growing exponentially. Regarding to that fact, the support from the IT aspect have to be followed as well, especially in data management. In fact, they are currently moving towards better management of data which is approaching centralized model. Since centralized model is vulnerable in system crash, malfunction, failure, even disaster, it is wisely to have a backup management process to prevent the loss of data caused by those.
Aside to prevent the loss of data, backup management process can also be used for archiving purpose. It is happened when the company want to keep old data without put the load on the current system's storage.

Looking at the global case, especially in small and medium business (SMB) market where the margin between the business to remain alive or close down is determined by the capacity of recovering from disaster, data lost can be somewhat costly if it is occurring. Critical data loss also will impact on the financial which also causes loss at the very least in companies of all all sizes. Based on the study of Computer Economics in 2002, In the first six months of 2001, American businesses lost over $8 billion due to data loss caused by computer viruses [1]. A combination of loss of business, low productivity, legal action, and the cost of re-creating data is the one which impacting the financial aspect. A survey from Symantec in 2009, regarding to information protection in SMB, shows that the cost spent caused by data loss is directly impacting financial cost and can be summarized as following [2]:

![Figure 1: Direct monetary impact caused by data loss based on Symantec](image)

At its worst, critical data loss can result in business collapse. Studies by the
National Archives and Records Administration showed that 80% of companies without well-conceived data protection and recovery strategies go out of business within two years of a major disaster [3]. The Ontrack survey in 2002 shows the following to be the most common causes of data loss [4].

![Figure 2: Causes of data loss based on Ontrack](image)

Back to the case in PLN Pusdiklat, currently, there is an approach to backup the data from servers. The approach might be said simple, and done quite manually. In general, they backup by manually copying the desired data into an external hard disk drive. It is still the best choice for them since actually there is no division specialized in IT. Therefore, this kind of approach which is simple, straight forward, and easy to operate is still preferable be done.

Despite of that simple approach, there are potential drawbacks. From efficiency aspect, that simplicity can turn to inefficient operation when the operator need to conduct data backup everyday from several directories from different servers. In fact, currently only data from 1 server is being backed-up due to that limitation. Another aspect is looking towards the security. Since the data is actually backed-up to a Windows-based
workstation, like any other of computer, it is reluctant to malware attack that might affect the data healthy. Last, there is a slight possibility of disaster, whether it is human error or natural disaster. Locating the backup disk in the same site along the servers could have catastrophic impact when a disaster struck the servers site.

It is essential to reengineer the backup management looking at those drawbacks from the current approach and considering common causes of data loss. The new mechanism should at least cover the weaknesses of the current system and suitable for the company. The efficiency aspect can be achieved through a scheduled, and automated backup process. To provide the security, the new system should have dedicated server in separate environment. Dedicated backup server also designated to deduct the possibility of hardware failure towards its reliability. And last, that server can be located in different location away from the servers site. As mentioned before, since there is no IT division, especially the one who specialized in IT networking or administration, the operation and admission process should be considerably easy due to the fact of human error place as a major cause of data loss.
1.2 Scope, Constraints, and Assumptions

1.2.1 Scope

From the problem exposed in the background, this field project will covers the implementation of a new backup system that suitable, efficient, and secure for the company. Suitable means considering whether the new system is fit for the company need and constraint. Efficient covers the need of effort in doing the backup operation. The security includes both of physical security where the data will be stored, and the safeness of the data to avoid (or minimize) the probability of data loss.

As a preceding action, it is expected to conduct research on what method and technologies will be implemented. Operating system, software packages, and hardware set are included in the consideration. To complement the work, analysis whether the work meet those requirement have to be conducted. The analysis can be in form of performance measure or satisfactory to check if it is brought a significant effect from the current system or not.

1.2.2 Constraints

As like any other field works, this project also have some constraint set by the company which force the design of the solution to be suitable with. The constraints here are fundamental which includes three of the following:

- **Time**: The system have to be implemented by the end of November 2010. The implementation by that time should cover basic feature of backing up data. Other feature enhancement and analysis can be done afterward.
• **Manpower**: No third party services or resources are allowed in the field work and further operation considering the sensitive corporate data that might involved. In fact, most of the work will be done by the author solely with support from colleagues. Lastly, there are no specific IT team, especially in network administration part, assigned as the user to operate the system and for further monitoring and maintenance.

• **Budget**: Regarding to the company's baseline, the project should spent at least Rp. 40 million and should not more than Rp. 80 million.

1.2.3 Assumptions

To ensure the completion of the field work, it is assumed that the company will fully support the activities. The support can be in forms of providing needed informations, incorporate in assisting the communication between divisions or branches, and supporting everyday operations.

1.3 Aims and Benefits

1.3.1 Aims

By achieving the advantage of implementing the new backup mechanism for the company which is having criteria explained in the scope covering suitability, efficiency, and security, the field work is intended to increase and improve the availability and safety of the data for the company. There is no such absolute solution to wipe out the risk of data loss, so in here the work is to minimize the risk of that.
1.3.2 Benefits

It is expected that the company's backup management would be more organized. By having well organized backup management, the company could have indirect benefit in form of effort saving for what they have been working for to produce the data. Another form of benefit is to maintain the operational efficiency that might lead to increasing productivity.

Aside from the company which getting direct benefits, the solution designed in this field work, whole, or partly, might assist other network administrator, or engineer in other companies to solve similar problem of managing backup.

1.4 Structure

This field work thesis will contain these following chapters which respect to general IT solution design methodology. The brief summary of the structure follows:

- **Introduction**

  The chapter is the beginning of the thesis. It tells the background of the company's ICT circumstances, expose the problem of the necessity of having proper backup management, point out the facts about data loss, and why the author need to make a change. After having a clear image of the problem, it defines the scope of the work, constraint from the both sides, and also assumptions made. Lastly, it also point out the aims and benefits achieved from this work.

- **Theoretical Foundation**

  The chapter mainly shows the definitions and concept of related terms of the
thesis topic. The approximation is to point out the concept about general data backup
definition, the classification of the data backup regarding to several aspects (i.e frequencies, scale, etc), the current example of enterprise backup software and hardware. To sum up, there will be comparison tables throughout sub-discussions.

- **Analysis on the Existing System**

  The chapter analyses in more detail about the current situation regarding IT infrastructure in PT Pusdiklat and other area involved, specifically how the existing backup mechanism used. It might shows the related existing topology or configuration. Then, It going to explain what the strengths and weaknesses of the current system. In addition, the analysis can show some numbers or satisfactory responses of the current performance as facts to support the exposure of the problem.

- **Solution Design**

  The chapter explains the concept, and how the proposed system will be work regarding to the result of the problem analysis. It will break down in more detail about what kind of backup method suits, needed hardware specification, installed software, and other related technologies. To depict it clearer, it might also shows the expected topology if there is any changes required. All of the aspect that proposed will be supported with own analysis and other people works.

- **System Implementation and Testing**

  The chapter explains about how to implement the system, starting from the simulation strategy up to the final deployment. This will also include the explanation of all configuration needed and operational procedure. Network topologies and
snapshots of the documentation might be involved to give a clearer picture.

- **Evaluation**

  The chapter evaluates how the system performed after the implementation. It can begin from the simulation result to have a sneak look on how the system will behave. If there is something wrong, the author should go back to the solution design phase and re-iterate it. Once the real system implemented, it should analyze whether it meet the requirement given and the significance of implementing the new solution.

- **Conclusion and Recommendation**

  The chapter concludes the main ideas of the work, including the problem, solution, implementation, and result. Based on the conclusion made, this thesis will be closed with recommendations about the work and how the system should improve for near or further future.