

## INTISARI

Penggunaan teknologi informasi sangat penting dan memiliki banyak pengaruh untuk kinerja pada perusahaan terlebih lagi pada proses bisnis serta keamanan data perusahaan. Namun, pada proses implementasi teknologi informasi tersebut dapat memungkinkan timbulnya berbagai macam risiko yang mengancam keamanan didalamnya. Jika diamati, hal yang sangat berpengaruh dalam perusahaan adalah kualitas sumber daya yang bekerja serta ancaman yang berasal dari pihak internal maupun eksternal. Keamanan pada perusahaan dapat terjamin jika pekerja dapat memiliki acuan dan pengetahuan tentang company security atau mengarah pada keamanan, baik meliputi keamanan data penting perusahaan atau keamanan secara fisik. Hal tersebut perlu diperhatikan agar perusahaan lebih waspada terhadap ancaman atau risiko yang terjadi. Perusahaan juga harus memperhatikan jenis serangan dan persyaratan keamanan seperti confidentiality, availability and integrity karena jika tidak melakukan usaha untuk keamanan tersebut dapat berakibat fatal bagi perusahaan. Contoh serangan pada data seperti virus, credential reuse, cross-site, cripting, password cracking dan pengaruh yang bisa didapatkan berupa destruction (penghancuran), discloure (penyingkapan), interruption (gangguan) serta kerugian secara reputasi dan finansial. Tujuan dari penelitian ini adalah memberikan sebuah rekomendasi pada CV Arta Rahmat Sejati Cilacap terhadap ancaman dan risiko yang terjadi menggunakan metode Octave Allegro. Penelitian ini adalah penelitian kualitatif yang bersifat deskriptif, juga cenderung menggunakan analisis dan penelitian kuantitatif yang bersifat sistematis untuk memberikan sebuah penilaian risiko, strategi keamanan informasi untuk evaluasi kerentanan. Hasil dari penelitian ini yaitu terdapat ancaman berupa hal yang berpotensi untuk melakukan pengeksploitasian celah keamanan diantaranya pada using technical means, human actor using physical means, technical problems dan hasil penilaian analisa risiko tertinggi sebesar 12 (high) pada impact area data security. Dari hasil keseluruhan menunjukkan aset informasi yang bersifat kritis sehingga membutuhkan upaya perencanaan untuk memberikan indikasi berupa penanganan, mitigasi risiko serta perubahan yang wajar dalam praktik keamanan pada perseroan komanditer tersebut.

Kata kunci: Manajemen Risiko, Teknologi Informasi, Company Security, Data Security

## **ABSTRACT**

*The use of information technology is very important and has a lot of influence on company performance, especially on business processes and company data security. However, in the process of implementing information technology, it can allow the emergence of various kinds of risks that threaten the security in it. If observed, the thing that is very influential in the company is the quality of the resources that work as well as threats from internal and external parties. Security at the company can be guaranteed if workers can have references and knowledge about company security or lead to security, whether it includes security of important company data or physical security. This needs to be considered so that companies are more aware of threats or risks that occur. Companies must also pay attention to the types of attacks and security requirements such as confidentiality, availability and integrity because if they do not make efforts for security, it can be fatal for the company. Examples of attacks on data are viruses, credential reuse, cross-site, crypting, password cracking and the effects that can be obtained in the form of destruction, disclosure, interruption and reputational and financial losses. The purpose of this study is to provide a recommendation to CV ARTA RAHMAT SEJATI CILACAP against threats and risks that occur using the Octave Allegro method. This research is a descriptive qualitative research, also tends to use systematic quantitative analysis and research to provide a risk assessment, information security strategy for vulnerability evaluation. The results of this study are that there are threats in the form of things that have the potential to exploit security vulnerabilities including using technical means, human actors using physical means, technical problems and the results of the highest risk analysis assessment are 12 (high) in the impact area of data security. The overall results show critical information assets that require planning efforts to provide indications in the form of handling, risk mitigation and reasonable changes in security practices at the limited liability company.*

*Keywords: Risk Management, Information Technology, Company Security, Data Security*



