Universiti Teknologi MARA

Securing IT Management in Organization

Nurmuzlifa binti Mohamad Munir

Thesis submitted in fulfillment of the requirements for
Bachelor of Science (Hons) Information Technology
Faculty of Information Technology And
Quantitative Science

April 2008

ACKNOWLEGEMENT

Firstly, I would like to pay my gratitude to Allah S.W.T for giving me strength to be able to complete this research paper. I would also like to express my appreciation to my supervisor, Assoc. Prof. Yap May Lin who has guided me in doing he research. Her guidance and supervision will undoubtedly help me in my future undertakings. I also like to convey my appreciation to my thesis coordinator, Pn. Rozianawaty for her guidance and advice in settling this research paper.

I would also like to convey my appreciation to my fellow friend Nurulshima Ahmad Bazthery, thank you for sharing information throughout the making of this research paper. Thanks to those who has also helped me indirectly or directly in completing this research paper.

TABLE OF CONTENTS

RESEARCH APPROACH AND METHODOLOGY

ABSTRACT

Information Technology (IT) deals with the uses of electronic computers and computer software to convert, store, protect, process, transmit and retrieve information. Information exists in many forms, and different types of information have different values to an organization. The impact of threats to confidentiality, integrity and availability of information also depends on the information and an organization's mission. As information systems become increasingly interconnected, the opportunities for compromises increase. This paper focuses is to determine secure IT management practices among organizations and their awareness level. It also elaborated on ISO 27001, currently the only auditable international standard that defines the requirements for ISMS. It helps to establish policies, objectives and controls for information security within the context of an organization's overall business. It is based on a methodical business risk approach to establish, implement, operate, monitor, review, maintain and improve information security. The findings concluded that that the awareness level of organization in securing their IT management is moderate. More than half of the respondents agree that insider threat posed more damage (40%) yet only 43% of respondent applies security training to new employee. This is may be because security executives and top management may be becoming over confident. Even though they are making serious headway in understanding and combating threat, organizations think they have things handled when most of them (70%) only review and update their security policy only as needed. More than half of the respondents agree that insider threat posed more damage (40%) yet only 43% of respondent applies security training to new employee.