An Assessment of ISMS Process Maturity based on Readiness and Awareness of team members of selected IT Organizations

Dr. Alpana Kakkar, Dr. Ritu Punhani

Dr. S. Madan, Dr. D. Jain

International Research Journal
ISSN 1839-6518
Vol. 2, No. 2, 2012
82800202201203

An Assessment of ISMS Process Maturity based on Readiness and Awareness of team members of selected IT Organizations

Dr. Alpana Kakkar,
Dr. Ritu Punhani
Dr. S. Madan, Dr. D. Jain

International Research Journal
ISSN 1839-6518
Vol. 2, No. 2, 2012
82800202201203

An Assessment of ISMS Process Maturity based on Readiness and Awareness of team members of selected IT Organizations

Abstract

The growth of computers and of information technology has been explosive. As a result, information technology has been widely applied in every aspect of our life—from business, government, education, finance, health-care, aerospace to national defence. Computers, especially networked computers, have brought benefits to us and improved our lives. However, surveys and reports from various industry associations and security organizations suggested that only a few organizations can successfully protect their information assets. Organizations realize that information security is a complex issue, involving both human and technical factors. This paper is an attempt to empirically assess the maturity of Information Security Management System (ISMS) implementation in selected IT Service organizations in terms of confidence of their employees on their Information Security Management System.

Keywords: ***ISMS, ITS, ITSM, ISO 9001, ITIL***

Introduction

The growth of computers and of information technology has been explosive. As a result, information technology has been widely applied in every aspect of our life—from business, government, education, finance, health-care, aerospace to national defence. Computers, especially networked computers, have brought benefits to us and improved our lives. However, surveys and reports from various industry associations and security organizations suggested that only a few organizations can successfully protect their information assets. Organizations realize that information security is a complex issue, involving both human and technical factors. Experience indicates that technology cannot provide all the answers to the security problems posed by people in the context of ISM. According to the CSI/FBI survey report, 89% organizations have firewalls and 60% use IDs, and yet 40% reported system intrusion from

outside of the organization (Power, 2002). This report also revealed that although 90% of organizations used anti-virus software, 85% were still hit by viruses, worms, etc.

To protect organizational information assets, many different information security standards and guidelines have been published. The two major sources for information security standards and guidelines are professional societies and the U.S. federal government. Generally Accepted System Security Principles (GASSP), for example, is a joint international effort between 10 countries worldwide to develop a set of rules, practices, and procedures to achieve information integrity, availability, and confidentiality. Federal Information Processing Standards Publications (FIPs PUBs) provide guidelines that are mandatory for government agencies, but optional for the private sector. The newly released international standard ISO17799 was aimed to provide a suitable model for information security management (ISM).

Unfortunately, the current information security measurement criteria and practices are inconsistent and very confusing, which can be misleading to practitioners. Moreover, current concepts in the field of ISM are based largely on case studies, anecdotal evidence and the prescription of industry "leaders". There is little consensus on which information security objectives should be achieved, which practices are critical to successful security initiatives, and what are the relationships between the "best practices" and information security objectives.

In order to effectively manage information security, the following fundamental issues must be addressed:

1. What is information security?
2. What are the objectives of information security and how is information security measured?
3. What kind of programs or practices can an organization implement to achieve these security objectives?
4. What management practices are perceived as critical by information technology professionals?
5. What are the underlying relationships between information security objectives and information security practices?

6. Specifically, which particular practice contributes to which specific security objective?
7. The lack of an existing framework to aid practitioners in implementing ISM practices.

Answers to these issues have practical implications given the importance of information security. Surprisingly, to our knowledge, there has been no scientific study conducted on synthesizing security management practices and mapping the relationships between these practices with information security objectives. For example, current frameworks such as ISO 17799/BS 7799, GASSP, ISO 13335, have not been validated by empirical research.

The purpose of this white paper is to make an attempt to empirically assess the maturity of Information Security Management System (ISMS) implementation in selected IT Service organizations in terms of confidence of their employees on their Information Security Management System.

Assessment based on Employee Confidence

Employees of an organization or members of any team are the true face of their internal strengths as well as weaknesses, doesn't matter someone accepts them or not. Relying on this management and psychological factor, we made attempt to conduct a survey about readiness and awareness of policies and processes related to Information Security Management System of selected sample organization.

Assessment foundation

The assessment is carried out based on the response of randomly selected employees of a set of IT organizations on a given set of nine point questionnaire where the response on each point of the questionnaire is captured on four options interface. This interface is formed with the following four options:

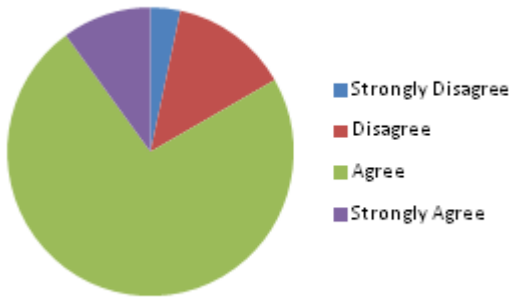
1. Strongly Disagree
2. Disagree
3. Agree
4. Strongly Agree

The nine points of the questionnaire are as follows:

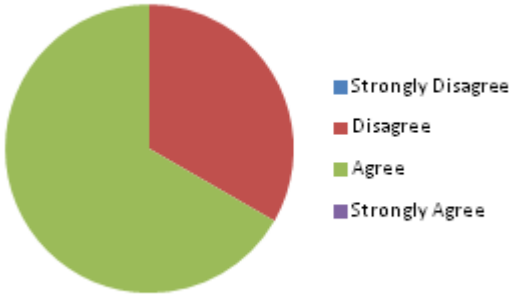
1. There exists a customer driven or customer influenced culture in our organization.
2. We have been trained on and we understand value additions to the customer through each of our services or work products.
3. Relevant metrics are been defined and used for measurement of quantity and quality of our services or work products.
4. The delivery and support processes are being adequately defined in our organization.
5. A common set of service support and delivery terminology is accepted and used across our organization (may be through some standard templates etc.).
6. Continuous improvement in our services or work products or delivery processes exists in culture of our organization.
7. The organization follows a culture of clearly defining the Roles and Responsibilities of all team members for any project or task.
8. Work items are clearly prioritized for their importance to accomplish in the projects.
9. Service/Work Support processes and policies of the organization are well documented and maintained with easy access for reference as and when required.

Survey Responses

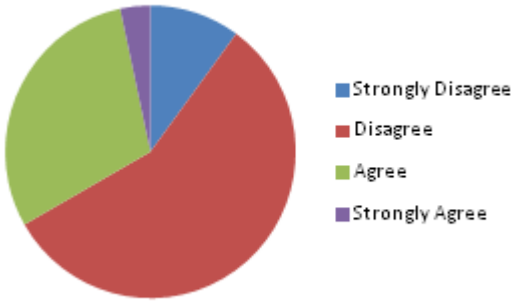
There exists a customer driven or customer influenced culture in our organization.		
1-Strongly Disagree	1	3.33%
2-Disagree	4	13.33%
3-Agree	22	73.33%
4-Strongly Agree	3	10.00%
Totals	**30**	**100%**



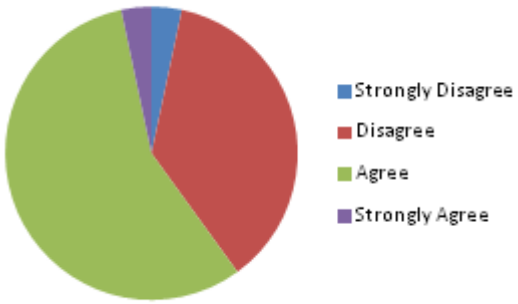
We have been trained on and we understand value additions to the customer through each of our services or work products.		
1-Strongly Disagree	0	0.00%
2-Disagree	10	33.33%
3-Agree	20	66.67%
4-Strongly Agree	0	0.00%
Totals	**30**	**100%**



Relevant metrics are been defined and used for measurement of quantity and quality of our services or work products.		
1-Strongly Disagree	3	10.00%
2-Disagree	17	56.67%
3-Agree	9	30.00%
4-Strongly Agree	1	3.33%
Totals	**30**	**100%**

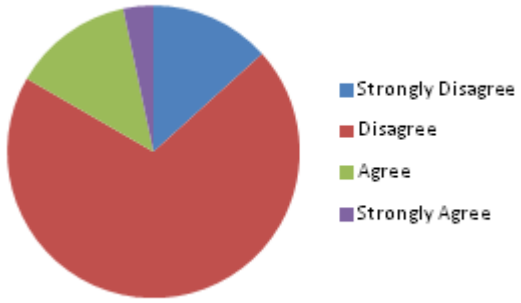


The delivery and support processes are being adequately defined in our organization.		
1-Strongly Disagree	1	3.33%
2-Disagree	11	36.67%
3-Agree	17	56.67%
4-Strongly Agree	1	3.33%
Totals	**30**	**100%**



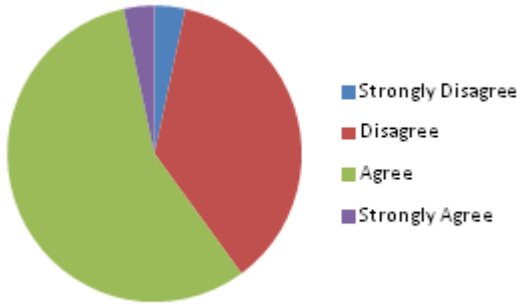
A common set of service support and delivery terminology is accepted and used across our organization (may be through some standard templates etc.).

1-Strongly Disagree	4	13.33%
2-Disagree	21	70.00%
3-Agree	4	13.33%
4-Strongly Agree	1	3.33%
Totals	**30**	**100%**



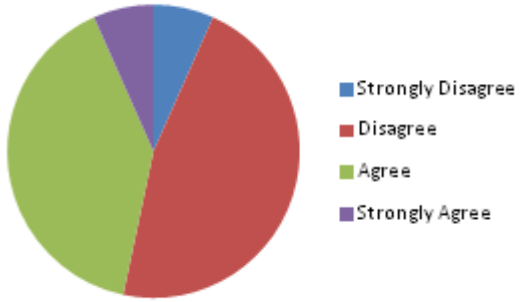
Continuous improvement in our services or work products or delivery processes exists in culture of our organization.

1-Strongly Disagree	1	3.33%
2-Disagree	11	36.67%
3-Agree	17	56.67%
4-Strongly Agree	1	3.33%
Totals	**30**	**100%**

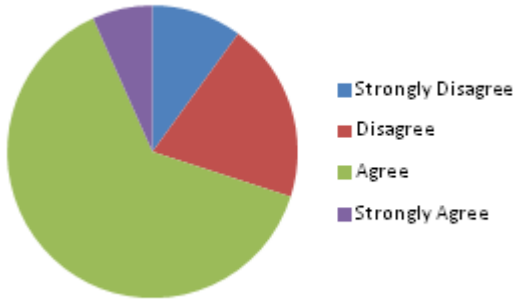


Organization has a culture of clearly defining the Roles and Responsibilities of all team members for any project or task.

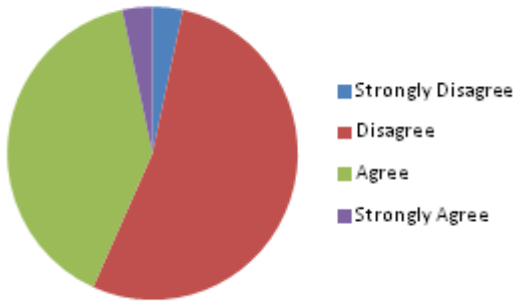
1-Strongly Disagree	2	6.67%
2-Disagree	14	46.67%
3-Agree	12	40.00%
4-Strongly Agree	2	6.67%
Totals	**30**	**100%**



Work items are clearly prioritized for their importance to accomplish in the projects.		
1-Strongly Disagree	3	10.00%
2-Disagree	6	20.00%
3-Agree	19	63.33%
4-Strongly Agree	2	6.67%
Totals	**30**	**100%**



Service/Work Support processes and policies of the organization are well documented and maintained with easy access for reference as and when required.		
1-Strongly Disagree	1	3.33%
2-Disagree	16	53.33%
3-Agree	12	40.00%
4-Strongly Agree	1	3.33%
Totals	**30**	**100%**



Analysis and Recommendations

The Readiness and Awareness assessment of ISMS policies and implementation in selected IT Service Organizations are showing the overall security falls slightly above the midpoint (2.50) on the readiness and awareness scale. Out of the selected nine points of the questionnaire, five points are above the center whereas the other four are below the center. This should also be noted that none of the point could score the responses towards the highest or lowest ends of the four point scale. Overall the responses are found to be balanced which in fact shows the presence of a base upon which an information security culture can be formed and the maturity can be attained or increased.

Looking into the responses provide by the participants, it can be seen that a fairly good acceptance is captured for presence of customer driven culture. More than three fourth of participants have rated either “agreed” or “strongly agreed” for presence of customer driven culture in their organization. According to management experts, the customer focus is usually considered beneficial for sustenance of business and success of organizations for better ISMS practices because while awarding any projects or work items to a company, the customer acts as an external and more concerned party for effectiveness of ISMS.

On the other side, the least score is found for acceptance of common set of service support and delivery terminology across the organization. It is found that more than three fourth of participants have rated either “Disagreed” or “Strongly Disagreed” if a common set of terminologies are accepted and used across organization. This in fact can be a risk in understanding of scope, processes, and other knowledge important for acceptance and implementation of ISMS in the organization.

References

1. Bachman, D. 2002. Information Systems Security: Principles and Perspectives. Sprint E| Solutions. White paper: 1-13.
2. Blackwell, E. 1998. Building a solid foundation for intranet security. Information Systems Management. Spring 15(2): 26-34.
3. Bostrom, R. and Heinen, J. 1977. MIS problems and failures: a socio-technical perspective - Part I: the causes. MIS Quarterly September: 17-32.
4. Bosworth, S. and Kabay, M. E. 2002. Computer Security Handbook (4th edition, Bosworth and Kabay eds.). New York, NY: John Wiley & Sons, Inc.
5. Brenner, B. 2005. Botnets are more menacing than ever. Retrieved September, 2005 from http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1068871.00.html
6. CMMI for Services, Version 1.2, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, 2009.
7. Executive Briefing: The Benefits of ITIL®, Maggie Kneller, ©The Stationary Office, 2010.

8. Fried, L. (1994). Information Security and New Technology Potential Threats and Solutions. Information Systems Management, 11 (3): 57-63.
9. Furnell, S. M., Papadaki, M., Magklaras, G. and Alayed, A. 2001. Security Vulnerabilities and System Intrusions: The Need for Automated Response Frameworks. In H. P. Eloff, L. Labuschage, R. V. Solms & G. Dhillon (Eds.), Advances in Information Security Management & Small Systems Security. Dordrecht, Netherlands: Kluwer Academic Publishers.
10. Gerth, A. B. and Rothman, S. 2007. The Future IS Organization in a Flat World. Information Systems Management. 24(2): 103-111.
11. GFOA (Government Finance Officers Association), 1997. An Introduction to Treasury Management Practices, GFOA, ISBN 0891252118, 65 pages.
12. Gordon, L. A. and Loeb, M. P. 2006. Budgeting process for Information Security Expenditures. Communications of the ACM. 49(1): 121 - 125.
13. Gordon, L. A., Loeb, M. P., Lucyshyn, W. and Richardson, R. 2005 CSI/FBI Computer Crime and Security Survey. Retrieved from www.gocsi.com/forms/fbi/csi_fbi_survey.jhtml;jsessionid=CREWIZUTIPCCSQSNDBCCKHSCJUMEKJVN
14. Host, R. 2001. New information security requirements for federal agencies. Accessed on Feb. 25, 2003 at: http://www.sans.org/rr/policy/fed.php
15. ITIL v3® Continual Service Improvement, Office of Government and Commerce, London: TSO, 2011.
16. ITIL v3® Service Design, Office of Government and Commerce, London: TSO, 2011.
17. ITIL v3® Service Operation, Office of Government & Commerce, London: TSO, 2011.
18. ITIL v3® Service Strategy, Office of Government and Commerce, London: TSO, 2011.
19. ITIL v3® Service Transition, Office of Government & Commerce, London: TSO, 2011.
20. ITIL®: The Basics, Valerie Arraj, © Official Accreditor of the OGC ITIL Portfolio: APM Group Limited, 2010.
21. Krause, M. and Tipton, H. F. 2002. Handbook of Information Security Management, CRC Press LLC, ISBN: 0849399475.
22. Kruger, H. A. and Kearney, W.D. 2006. A prototype for assessing information security awareness. Computers & Security. 25(4): 289 - 296.

23. Pant, S. and Hsu, C. 1999. An integrated framework for strategic information systems planning and development, Information Resources Management Journal. 12(1): 15 - 25.
24. Paulk, M.C., Curtis, B., Chrissis, M.B. and Weber. C.V. 1993. Capability Maturity Model for Software, Version 1.1 Technical Report. CMU/SEI-93-TR-024, ESC-TR-93-177. Retrieved from: http://www.dynamics.unam.edu/NotasVarias/CMM.pdf
25. Peltier, T. R. 2003. Preparing for ISO 17799. Security Management Practices. 21 - 28.
26. Porter, M. and Millar, V. 1985. How information gives you competitive advantage. Harvard Business Review. July-August: 149 - 160.
27. Reich, B.H. and Benbasat, I. 2000. Factors that influence the social dimension of alignment between business and information technology objectives. MIS Quarterly. 24(1): 81 - 111.
28. Straub, D. W. and Welke, R. J. 1998. Coping with systems risk: security planning models for management decision making. MIS Quarterly 22(4): 441 - 469.
29. US-CERT, United States Computer Emergency Response Team. Retrieved May 2006 from http://www.us-cert.gov/reading_room/brochure_securityguidance.pdf.
30. Wright, M. A. 1994. Protecting information: effective security controls. Review of Business, 16(2): 4 - 9.
31. Zviran, M. and Haga, W. J. 1999. Password security: an empirical study. Journal of Management Systems, 5(4): 161 - 185.

- END -

Certificate of Recognition

This certificate is awarded to

Alpana Kakkar

in recognition of her contribution

"An Assessment of ISMS Process Maturity
based on Readiness and Awareness of team members
of selected IT Organizations"

to Vol. 02, No. 02, 2012 *of*

IARS International Research Journal

Editor in Chief

IARS International Research Journal
29 AUG 2012