Information Risk Management: The Current Challenges Faced by Organizations and their Solutions

Description: Information Risk Management has become a mission critical business requirement for businesses across the world amidst known and emerging threats facing the Information Systems of organizations. A lot of action is carried out in this area with loads of products & services introduced in the global markets and billions of dollars being burnt by business owners. But everyone has one question in their minds – are we doing enough? Business owners want to know whether they are effectively & proactively identifying the information risks and implementing adequate controls to mitigate them. This paper presents the problems faced by global organizations pertaining to Information Risk Management and presents solutions that are deemed feasible by a number of respondents that participated in a survey of 325 participants conducted by the researcher. If the Risk Management and Information Security consulting companies across the world design service packages to “implement the frameworks and not only advise on them” to the extent that they are culturally accepted by the employees and the value addition to business is tangibly demonstrated, they can tap a huge market potential across the globe. As per estimates carried out in this research the Information Security and Risk Management markets in the technology & knowledge intensive sectors of UK and all countries under European Union put together offer a market potential of about $12 Billion for one time implementation and about $1.5 Billion in annual service charges if the Information Security and Risk Management consultants package and offer the services designed in this report.

The target audience of this report are:
- IRM professionals practicing in the global markets
- External and Internal auditors
- Senior Management, Top Management & Board members of organizations that either have IRM implemented or are planning to implement in due course
- IRM & ISMS process package and software tool design companies
- Quality Management professionals
- IT Security & ISMS professionals
- Legal & Statutory strategy makers
- IRM managers in Government & Public Sector units

Some of the key findings of the report are:
- The IRM & ISMS training manuals for employees mostly comprises of checklists of dos and don'ts whereby very little emphasis is given on improving the general knowledge of employees on the threats and associated impacts. The knowledge management efforts for employees pertaining to IRM & ISMS as a subject matter or domain area is not adequate.
- The security policies & acceptable usage policies written in the organizations as an outcome of IRM are more of “compliance enforcement documents” describing breaches and punishments very much in detail but not giving much emphasis on the rationale of the controls although it should be other way round. In fact these documents are the most uninteresting papers to be read by employees and most of the time responsible to induce fear psychosis and play safe attitudes in organizations.
- Very little efforts are applied to achieve buy in of employees on the security controls by understanding the negative impacts from them and modifying the documented policies to make them optimal from management and employee perspective.
- Implementation of stringent security controls have resulted in reduction of employee satisfaction & innovation capability thus resulting in reduction of delivery efficiency and effectiveness of the organization.
- The IRM and ISMS teams normally sit outside the IT & IS functions having members that are not qualified & experienced to carry out in depth audit of the technical environment of the organization. Thus, the auditing of these functions becomes more of paperwork to satisfy the audit plan requirements.

Contents:

ABSTRACT

1.0 INTRODUCTION:
1.1 RESEARCH OBJECTIVES AND THE RESEARCH QUESTIONS
1.2 SIGNIFICANCE OF THE REPORT
1.3 HYPOTHESES OF THE REPORT
1.4 SCOPE AND LIMITATIONS OF THE REPORT
1.5 THE PROPOSED OUTPUT OF REPORT

2.0 LITERATURE REVIEW AND DISCUSSIONS
2.1 GLOBAL BEST PRACTICES IN INFORMATION RISK MANAGEMENT
2.1.1 NIST RECOMMENDATIONS:
2.1.2 THE ISO 27002:2008 STANDARD:
2.1.3 THE ISO 27005:2008 STANDARD:
2.1.4 THE COBIT FRAMEWORK:
2.1.5 CRAMM, OCTAVE AND FRAP FRAMEWORKS:
2.2 THE CURRENT CHALLENGES IN INFORMATION RISK MANAGEMENT AND THEIR SOLUTIONS
2.2.1 INFORMATION ASSET MANAGEMENT
2.2.2 EVALUATION OF ASSET VALUE
2.2.3 ANALYSIS OF EXPOSURE OF ASSETS TO KNOWN AND EMERGING THREATS
2.2.4 ANALYSIS OF IMPACT TO THE BUSINESS, CUSTOMERS, REPUTATION AND FINANCIALS
2.2.5 REGULATORY IMPACT ANALYSIS
2.2.6 ANALYSIS OF PROBABILITY OF OCCURRENCE
2.2.7 ANALYSIS OF INTERNAL VULNERABILITIES
2.2.8 CONCLUDING THE RISK VALUES
2.3 FORMULATION AND APPLICATION OF CONTROLS – CHALLENGES AND SOLUTIONS
2.3.1 THE CONTROLS FRAMEWORK OF ISO 27001:2005
2.3.2 APPLICATION OF CONTROLS
2.3.3 TESTING THE EFFECTIVENESS OF CONTROLS
2.3.4 MANAGEMENT COMMITMENT TO INFORMATION RISK MANAGEMENT
2.4 CONTINUOUS IMPROVEMENTS – CHALLENGES AND SOLUTIONS
2.4.1 UPDATING THE THREAT DATABASE
2.4.2 KNOWING ADDITIONAL VULNERABILITIES
2.4.3 ENHANCEMENT OF EXISTING CONTROLS
2.4.4 CULTURAL ACCEPTANCE OF RISK MANAGEMENT FRAMEWORK
2.4.5 HIRING EXTERNAL CONSULTANTS AND AUDITORS

3.0 METHODOLOGY:
3.1 RESEARCH METHODOLOGY
3.2 RESEARCH LIFE-CYCLE
3.3 RESEARCH PROCEDURE
3.4 DECLARATION OF ETHICAL PERSPECTIVE
4.0 THE RESEARCH OUTPUT
4.1 OUTCOME OF THE PROJECT
4.2 SUMMARY OF RESULTS
4.3 CRITICAL DISCUSSIONS
4.4 CONCLUSIONS AND GENERALIZATIONS

REFERENCE LIST

List of Tables
Table 1: Template to prepare Statement of Applicability in ISO 27001 implementation
Table 2: Control Effectiveness Rating process to test vulnerability values as per BS ISO/IEC 27001:2005 standard
Table 3: Summary of responses from the respondents captured during the interviews

List of Figures
Figure 1: The Nine Step Risk Assessment Process recommended by NIST (Source: NIST Special Publication. 800-30. 2002)
Figure 2: Concentric Spheres Model of Risk Management Framework (Source: ISO 27005 conceptual framework)
Figure 3: Relationships in a Risk management Framework (Source: Conceptual framework of ISO 27005 standard)
Figure 4: Various databases maintained in the relationship model of Risk Management Framework (Source: Conceptual framework of ISO 27005 standard)
Figure 5: Focus Areas of IT Governance (COBIT Framework 4.1 by IT Governance Institute. 2007)
Figure 6: Input-Output framework of IT Risk Management (COBIT Framework 4.1 by IT Governance Institute. 2007)
Figure 7: Matrix Structure to evaluate Risk Value from Threat Value, Vulnerability Value and Asset Value
(Based on guidelines of ISO 13335-3 which is now ISO 27005)
Figure 8: An example of a Risk Heat Chart (Showing risks in absolute GREEN, AMBER, RED and those that are on the boundary)
Figure 9: The research life cycle followed in this report

Ordering:
Order Online - http://www.researchandmarkets.com/reports/1083024/
Order by Fax - using the form below
Order by Post - print the order form below and send to

Research and Markets,
Guinness Centre,
Taylors Lane,
Dublin 8,
Ireland.
Fax Order Form
To place an order via fax simply print this form, fill in the information below and fax the completed form to 646-607-1907 (from USA) or +353-1-481-1716 (from Rest of World). If you have any questions please visit
http://www.researchandmarkets.com/contact/

Order Information
Please verify that the product information is correct and select the format(s) you require.

Product Name: Information Risk Management: The Current Challenges Faced by Organizations and their Solutions
Web Address: http://www.researchandmarkets.com/reports/1083024/
Office Code: SCDV2GGA

Product Formats
Please select the product formats and quantity you require:

<table>
<thead>
<tr>
<th>Quantity</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Hard Copy:</td>
<td>USD 84 + USD 28 Shipping/Handling</td>
</tr>
<tr>
<td>CD-ROM:</td>
<td>USD 84 + USD 28 Shipping/Handling</td>
</tr>
<tr>
<td>Electronic (PDF) - Enterprisewide:</td>
<td>USD 84</td>
</tr>
</tbody>
</table>

* Shipping/Handling is only charged once per order.

Contact Information
Please enter all the information below in BLOCK CAPITALS

Title:  
Mr [ ]  Mrs [ ]  Dr [ ]  Miss [ ]  Ms [ ]  Prof [ ]
First Name: ______________________  Last Name: ______________________
Email Address: * ______________________
Job Title: ______________________
Organisation: ______________________
Address: ______________________
City: ______________________
Postal / Zip Code: ______________________
Country: ______________________
Phone Number: ______________________
Fax Number: ______________________

* Please refrain from using free email accounts when ordering (e.g. Yahoo, Hotmail, AOL)
Payment Information

Please indicate the payment method you would like to use by selecting the appropriate box.

☐ Pay by credit card: You will receive an email with a link to a secure webpage to enter your credit card details.

☐ Pay by check: Please post the check, accompanied by this form, to:
Research and Markets,
Guinness Center,
Taylors Lane,
Dublin 8,
Ireland.

☐ Pay by wire transfer: Please transfer funds to:
Account number 833 130 83
Sort code 98-53-30
Swift code ULSBIE2D
IBAN number IE78ULSB98533083313083
Bank Address Ulster Bank,
27-35 Main Street,
Blackrock,
Co. Dublin,
Ireland.

If you have a Marketing Code please enter it below:

Marketing Code: ____________________________

Please note that by ordering from Research and Markets you are agreeing to our Terms and Conditions at http://www.researchandmarkets.com/info/terms.asp

Please fax this form to:
(646) 607-1907 or (646) 964-6609 - From USA
+353-1-481-1716 or +353-1-653-1571 - From Rest of World