|  |  |  |
| --- | --- | --- |
| [ISO27001security logo 150](http://www.iso27001security.com/)   |  | | --- | |  | |  |
|  | **ISO27k Toolkit** |
|  | **Information security risk assessment** |
|  | **Released by the ISO27k Forum at www.ISO27001security.com** |
|  | **Version 3 August 2010** |
|  | **Introduction and purpose** |
|  | This spreadsheet is intended to support an organization's analysis of information security risks as part of the design and/or review of its Information Security Management System (ISMS). The spreadsheet is meant to help those implementing or planning to implement the ISO/IEC information security management standards, and to guide management.  Like the ISO/IEC standards, it is generic and needs to be tailored to your specific requirements.  The details do vary between organizations. |
|  | This is a **decision support tool**, not an objective, scientific analytical method, so it is important that users are skilled and competent in this area. |
|  |  |
|  | **History and acknowledgements** |
| v1 | The initial version of this spreadsheet was kindly contributed to the ISO27k Forum at www.ISO27001security.com by Hamid Nisar, along with a separate Word document explaining the scores and formulae, in 2007. |
| v2 | Hamid's spreadsheet and document were crunched into a multi-page spreadsheet by Gary Hinson, with minor changes to the wording and formatting, plus an introduction section. It was released in the free ISO27k Toolkit as version 2 in 2007. |
| v3 | The spreadsheet was modified and used by Bob Ralph in connection with the implementation of a management system for personal data. Bob's modified version was expanded and made generic by Gary Hinson, then republished and added to the free ISO27k Toolkit in 2010. |
|  | *Further improvement suggestions are very welcome from those actively implementing the ISO/IEC 27000 standards : please join the ISO27k Forum through www.ISO27001security.com and post your comments or updates to the group. Other ISMS documents, worksheets, policies, procedures etc. are very welcome too!* |
|  |  |
|  | **Copyright** |
|  | This work is copyright © 2010, ISO27k Forum, some rights reserved. It is licensed under the Creative Commons Attribution-Noncommercial-Share Alike 3.0 License. You are welcome to reproduce, circulate, use and create derivative works from this provided that: (a) it is not sold or incorporated into a commercial product, (b) it is properly attributed to the ISO27k Forum at www.ISO27001security.com, and (c) if shared, derivative works are shared under the same terms as this. |
|  |  |
|  | **References** |
|  | ISO/IEC 27005:2008 Information technology -- Security techniques -- Information security risk management (see ISO27001security.com for more info) |
|  |  |
|  | **Disclaimer** |
|  | Risk analysis is more art than science. Don't be fooled by the numbers and formulae: the results are heavily influenced by the accuracy of the users' assessment of risk factors, on the definition of information assets and on the framing of risks being considered. For these reasons, the process is best conducted by a team of people with solid expertise and practical experience of (a) assessing and managing information security risks, and (b) the organization, its internal and external situation with respect to information security. Don't expect to get definitive answers from anyone. It is impossible to guarantee that all risks have been considered and analyzed correctly. Some very experienced practitioners in this field claim that all risk analysis is basically bunkum, and we have some sympathy with that viewpoint. |
|  | The results of the analysis should certainly be reviewed by management (ideally including IT auditors, Legal, HR, other support functions and/or information security consultants) and may be adjusted according to their experience, so long as the expert views are taken into consideration. Remember: just because the organization has little if any experience of a particular information security risk does not necessarily mean that it can be discounted. Organizations with immature security management processes and systems may have significant ongoing security incidents that are not even recognized, due to inadequate incident detection and reporting processes. |

|  |  |
| --- | --- |
|  |  |
| **How to use the spreadsheet** | |
|  |  |
|  | The analysis looks at "information assets" which may be significant/valuable individual items or groups of related items, so start by listing them. |
|  | It may help to start with the register of information assets. |
|  |  |
|  | Now consider each asset in turn to determine the information security threats of some concern. It helps to think of types of possible incident. |
|  | Next consider the vulnerabilities, that is known weaknesses or flaws in the asset or the related processes etc. that might be exploited. |
|  | Next consider the possible impacts if the threats were to materialize and exploit the vulnerabilities, causing actual incidents. Think worst case. |
|  | Use the embedded heading cell comments to determine the scoring values you assign. Putting suitable numbers in those cells generates the raw risk level. |
|  |  |
|  | Some incidents are inherently difficult to identify, meaning they may continue unnoticed for some time, accumulating losses as they go. So, next rate the detectability. |
|  | That gives an overall risk score. |
|  | In the example spreadsheet, we have calculated the mean risk scores for each asset to help rank them - you may choose to do this differently. |
|  |  |
|  | Do this systematically to build up a picture of the risks. |
|  |  |
|  | From time to time, review the risk scores by eye to identify possible anomalies - scores that seem significantly higher or lower than were anticipated. |
|  | Review the data that gave such anomalous scores and add notes to confirm or doubt them. |
|  | Check the arithmetic: make sure the formulas are using data from the correct cells. |
|  |  |
|  | When the data stabilizes, rank (sort) the risks by overall risk scores, and use this as the basis for management decisions around acceptable risks, control requirements etc. |
|  | Maintain the spreadsheet thereafter and periodically re-check/refresh it to look for unacceptable risks that emerge. |
|  |  |
|  |  |
|  |  |
|  | *Note: we have left some example information in the spreadsheet to show how we envisage it being used. Please replace it with your own!* |
|  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Information asset** | **Known or suspected threats** | **Known or suspected vulnerabilities** | **Primary concerns (C/I/A)** | **Possibility of occurrence** | **Impact level** | **Raw risk level** | **Key information security controls in effect** | **Incident undetectability** | **Detected risk level** | **Mean risk total** | **Comments, notes, explanation** |
| **Database X** | Hacking | Internet connectivity; inadequate firewall protection | C + I | 1 | 3 | **3** | Data protection policies & procedures; network security controls; system security controls | 3 | **9** | **10** |  |
| Poor quality data | Poor quality information provided; incomplete checking and updating | A + I | 3.5 | 2 | **7** | Built-in integrity checks; routine procedures for checking & correcting data; ad hoc re-checks | 2 | **14** |  |
| Social engineering | Limited compliance with procedures; lack of awareness of the threat | C | 0.5 | 3 | **1.5** | Data protection policies & procedures; ongoing awareness program | 4 | **6** |  |
| **Web system Y** | Hacking | Internet connectivity; inadequate firewall protection; web client | I + A | 1 | 3 | **3** | Network security controls; system security controls; data security controls | 2 | **6** | **11** |  |
| Social engineering | Limited compliance with procedures; lack of awareness of the threat | C | 1 | 4 | **4** | Data protection policies & procedures; network security controls; system security controls | 4 | **16** |  |
| **LAN** | Hacking | inadequate firewall protection;Internet connectivity | A + I | 1 | 4 | **4** | network security controls; system security controls; data security controls | 3 | **12** |  |  |
| Virus, worm, trojan or other malware | internet connectivity;low security;inadequate firewall protection | C+I+A | 2 | 4 | **8** | network security controls; system security controls; data security controls | 3 | **24** |  |  |
| Data or system corruption | low security;internet connection;user system access overload | A + I | 3 | 4 | **12** | login controls;network security controls | 1 | **12** |  |  |
| **Backup tapes** | Theft | low security | A+C+I | 1 | 3 | **3** | security controls | 1 | **3** |  |  |
| Accidental or criminal damage, sabotage | low security | A+C | 3 | 3 | **9** | security controls | 1 | **9** |  |  |
| Fire, flood | low security;environment issues; | C+A | 1 | 4 | **4** | security controls;envirnmental controls | 1 | **4** |  |  |
| **PC's, laptops, PDAs etc. used by staff** | Theft | low security | C+I+A | 2 | 4 | **8** | security controls | 1 | **8** |  |  |
| Accidental or criminal damage, sabotage | low security;unexperienced access | C+A+I | 4 | 4 | **16** | security controls;employee training | 2 | **32** |  |  |
| **Servers** | Theft | low security | C+A+I | 0.5 | 4 | **2** | security control | 1 | **2** |  |  |
| Accidental or criminal damage, sabotage | low security;unexperienced access | C+A+I | 2 | 4 | **8** | security controls;employee training | 1 | **8** |  |  |
| Fire, flood | low security;environment issues; | C+I+A | 0.5 | 3 | **1.5** | security controls;envirnmental controls | 1 | **1.5** |  |  |