Desarrollando una metodología de análisis de riesgos para que el sector asegurador pueda tasar los riesgos en las PYMES

Antonio Santos-Olmo
Departamento de I+D+i
SICAMAN NT
Tomelloso, España
Email: Asolmo@sicaman-nt.com

Luis Enrique Sánchez
Departamento Eléctrica
y Electrónica
Universidad de las Fuerzas
Armadas Latacunga, Ecuador
Email: luisenrique@sanchezcrespo.org

Eduardo Fernández-Medina, Mario Piattini
Grupos de Investigación
ALARCOS y GSyA
Universidad de Castilla-La Mancha (UCLM)
Ciudad Real, España
Email: Eduardo.FdezMedina, Mario.Piattini@uclm.es

***Resumen*—En una sociedad gobernada por la información, las empresas y en particular las PYMES, dependen cada vez más de la capacidad de poder asegurar la información, no solo internamente, sino con terceros que estén dispuestos a establecer pólizas de seguros sobre la información. Pero cuando estamos hablando de activos intangibles, las aseguradoras se enfrentan a la problemática de que no existen metodologías de Análisis de Riesgos adecuadas que permitan tasar y garantizar la información de forma objetiva. En este artículo, presentamos la base de una nueva metodología que tiene como objetivo dar solución a las problemáticas presentadas por las empresas y las aseguradoras, permitiendo realizar un análisis de riesgo con menor grado de incertidumbre que los existentes en la actualidad.**

***Palabras clave*—PYMES; Analisis de riesgos; Tasación de activos; Aseguradoras**

I. Introducción

Para las empresas, es muy importante implantar controles de seguridad que les permitan conocer y controlar los riesgos a los que pueden estar sometidas [1], [2]. Pero la implantación de estos controles no es suficiente, siendo necesarios sistemas que gestionen la seguridad a lo largo del tiempo, de modo que les permitan reaccionar ágilmente ante nuevos riesgos, vulnerabilidades, amenazas, etc. [3]. Sin embargo, la mayor parte de las empresas tienen sistemas de seguridad caóticos creados sin unas guías adecuadas, sin documentación y con recursos insuficientes [4]. Los controles clásicos se muestran por sí solos insuficientes para dar unas mínimas garantías de seguridad. Por lo tanto, a pesar de que la realidad ha demostrado que para que las empresas puedan utilizar las tecnologías de la información y las comunicaciones con garantías es necesario disponer de guías, métricas y herramientas que les permitan conocer en cada momento su nivel de seguridad y las vulnerabilidades que aún no han sido cubiertas [5], el nivel de implantación con éxito de estos sistemas realmente es muy bajo. Este problema se acentúa especialmente en el caso de las PYMES, que cuentan con la limitación adicional de no tener recursos humanos y económicos suficientes para realizar una adecuada gestión [4]. Algunos autores [6], [7] sugieren la realización de un análisis de riesgos como parte fundamental en la PYME. Otros autores [8] proponen la necesidad de desarrollar un nuevo modelo de análisis de riesgos orientándolo directamente a las PYMES, considerando que el uso de técnicas de análisis y gestión de riesgos, así como el papel de terceros (Ej: aseguradoras), es necesario para poder garantizar la seguridad del sistema de información de las PYMES Como tal, toma especial relevancia la necesidad de obtener nuevas metodologías y modelos de análisis y gestión del riesgo, que permitan adaptarse a las PYMES, con el objetivo de eliminar (o al menos reducir) los inconvenientes y ayudar a estas sociedades a evaluar los riesgos a los que sus activos están expuestos y a establecer los controles de seguridad adecuados, permitiendo a su vez que esa evaluación de riesgos sea lo suficientemente objetiva, como para ser aceptada por terceros. De esta manera, el objetivo principal de este artículo es mostrar el framework que se está desarrollando con el objetivo de poder obtener una metodología de análisis de riesgos que dé solución a los problemas detectados en las investigaciones previas [9]. El artículo continúa en la sección II, describiendo brevemente el objetivo de la metodología y la problemática que pretende solucionar. En la sección III se presentan brevemente las propuestas de framework de la metodología. Finalmente, en la sección IV concluimos indicando cuál será el trabajo que desarrollaremos en el futuro.

II. Estado del arte

MARISMA (Metodología para Análisis de Riesgos SIstemático basado en Modelos Asociativos inteligentes y cuantificables) es la metodología que se está desarrollando con el fin de permitir la tasación objetiva de un sistema de información y la generación de un análisis de riesgo objetivo que tenga en cuenta aspectos asociativos y jerárquicos y sea de bajo coste en su generación y mantenimiento. Antes de iniciar la elaboración de MARISMA, se realizo una revisión sistemática siguiendo el método científico, que fue mostrada en la anterior edición de la RECSI [9], y de la que entre otros resultados se pueden destacar las siguientes conclusiones:

ISBN: 978-84-9717-323-0

1. La mayor carencia detectada en las metodologías actuales es el elevado nivel de aspectos subjetivos que deben ser establecidos y que invalida los resultados obtenidos, o por lo menos limita su uso [9]. A lo largo de nuestra experiencia hemos comprobado que la elaboración de un análisis de riesgos por parte de dos consultores, sobre la misma compañía, utilizando la misma metodología y con los mismos interlocutores, puede dar dos resultados completamente diferentes, al entrar en juego muchos aspectos subjetivos que deben ser valorados según la experiencia y el criterio de los consultores. Esta problemática hace que los resultados obtenidos en un análisis de riesgos sean parcialmente útiles para la propia compañía, pero totalmente inútiles cuando hablamos de terceras partes (compañías asociadas, proveedores, clientes, aseguradoras).
2. La segunda carencia detectada en las metodologías actuales, es que actualmente las metodologías consideran que las empresas y los activos están aislados. En base a nuestra experiencia de auditoría y certificación con la norma ISO27001 [10], nos hemos dado cuenta que uno de los mayores puntos de polémica es la definición del .ªlcance a certificar", ya que obliga a establecer una frontera clara de qué activos están dentro del alcance y cuáles no. Estos aspectos de asociatividad y jerarquía deben ser contemplados en un análisis de riesgos para que los resultados tengan un valor real y adecuado.
3. La tercera carencia detectada es la falta de un sistema de tasación monetaria adecuado para los activos de información. En reuniones mantenidas con aseguradoras, se llegó a la conclusión de que, en la era del conocimiento, una de las pocas cosas que todavía no podían asegurarse y que suponían un mayor riesgo para las compañías eran los sistemas de información, y que aunque cada vez más compañías solicitaban el poder asegurar y tasar el sistema de información, las compañías no habían localizado ningún mecanismo objetivo que les permitiera asegurar una compañía con las garantías necesarias.
4. La cuarta carencia detectada es que la metodología que se construya debe adaptarse a las características requeridas por las PYMES, que principalmente exigen un bajo coste de recurso, tanto económicos, como de tiempo y personal.
5. Finalmente, la quinta y última carencia detectada es que actualmente las empresas desconocen las inter-relaciones de sus activos con sus clientes y proveedores, carecen de ese grafo, lo que hace que les sea difícil entender muchas veces los riesgos que asumen. Aquí introducimos un nuevo concepto que creemos que puede llegar a solucionar ese problema y que es el concepto de Red Social Empresarial.ªplicada al control y la gestión de las inter-relaciones entre los activos de las compañías derivados de sus estructuras empresarial, o de la aprobación de un proyecto.

La metodología propuesta resolverá todas estas carencias detectadas durante la investigación, buscando que los resultados obtenidos sean no sólo validos desde el punto de vista científico, sino que tengan una aplicación directa a las empresas objetivo de la investigación.

III. FRAMEWORK MARISMA

El principal objetivo de esta investigación es el desarrollo de un marco de trabajo metodológico que permita realizar análisis de riesgos con el menor grado de incertidumbre, que sean válidos para las PYMES, que sean dinámicos, controlen aspectos asociativos y jerárquicos y permitan la tasación económica y objetiva de los Sistemas de Información de una compañía.

De cara a hacer posible la obtención de una valoración económica objetiva de un sistema de información y de los riesgos a los que están sometidos estos activos, con el menor grado de incertidumbre, con el objetivo de permitir a una compañía aseguradora poder realizar un seguro del mismo, o permitir conocer a un tercero los riesgos que asume al ceder un activo o colaborar con la compañía, planteamos la necesidad de desarrollar un marco metodológico que permita realizar este proceso.

El marco metodológico estará formado por tres componentes:

- *MI*: Contendrá el modelo de información, y estará formado por las ontologías y las bases de conocimiento del marco metodológico.
- *I*: Contendrá todas las métricas que nos permitirán las tasaciones económicas objetivas de los activos, y las reducciones del nivel de incertidumbre en la elaboración del análisis de riesgos.
- *M*: Contendrá la propia metodología de tasación y análisis y gestión del riesgo.

En las siguientes sub-secciones se irán detallando los principales elementos y características del marco de trabajo que se está desarrollando.

Modelo de Información - MARISMA.MI

La primera parte del marco metodológico que proponemos, contendrá un modelo de información que recoge todos los conceptos relacionados con la metodología que se pretende desarrollar. Estará formada por un conjunto de ontologías y una base de conocimiento, que nos permitirá reutilizar el conocimiento adquirido en diferentes implantaciones, y que estará basada en las investigaciones realizadas por [11], [12], entre otras.

Para el desarrollo de estas ontologías, debemos ser capaces de analizar las tres dimensiones del problema:

- *Conceptos relacionados con el campo de la tasación de activos (TA)*: para abarcar este dominio del problema, analizaremos otras investigaciones y estándares existentes. Las investigaciones realizadas hasta el momento han concluido que existen muy pocos estudios y estándares relacionados con la materia [13], [14].

- *Conceptos relacionados con el campo de la seguridad (S)*: para abarcar este dominio del problema, utilizaremos los principales estándares relacionados con la gestión de la seguridad de Sistemas de Información, en especial los relacionados con el análisis y gestión de riesgos (ISO27001, ISO27002, ISO27005, MAGERIT, OCTAVE, ...) [10], [15]–[24] y orientados en especial a disminuir el nivel de incertidumbre de la generación de un análisis de riesgos .
- *Conceptos relacionados con la interrelación de compañías (asociatividad y jerarquía) (AJ)*: para abarcar este dominio del problema, y ante la ausencia de estándares oficiales, utilizaremos los estudios obtenidos durante la revisión sistemática, que serán complementados con los resultados prácticos obtenidos de aplicar la investigación en caso reales mediante el método científico "investigación en acción".

El conjunto resultante de analizar estos tres dominios sobre un campo común como son los sistemas de información, dará lugar a un conjunto de ontologías que podremos aplicar sobre la metodología que estamos desarrollando.

Indicadores - MARISMA.I

La segunda etapa para el desarrollo de nuestra metodología se está centrando en el estudio y desarrollo de un conjunto de indicadores, reglas de negocio y métricas vinculadas a los procesos seguridad de los sistemas de información.

Uno de los objetivos de esta fase es facilitar que pueda determinarse de forma semiautomática la valoración (tanto monetaria como en cuanto a importancia dentro de la empresa) de los activos del sistema de información.

Una vez que hemos desarrollado la primera fase del marco de trabajo y obtenida una ontología, ésta se utilizará entre otras cosas para obtener reglas del sistema de tasación. Por último, estas reglas se utilizarán para aplicar factores derivados de las posibles relaciones de cada activo, amenaza y vulnerabilidad en cuanto a la jerarquía y asociatividad de la compañía dentro de su entorno, buscando siempre reducir el nivel de incertidumbre.

El objetivo último perseguido en esta fase es ser capaces de localizar y desarrollar indicadores y métricas que nos permitan calcular de forma semi-automática los valores de los activos y el nivel de riesgo al que están expuestos, reduciendo el nivel de incertidumbre en la elaboración del análisis de riesgos. De esta forma, esta parte de la investigación permitirá la consecución completa de los siguientes objetivos: i) Diseñar métricas para la valoración y tasación de activos de información; ii) Diseñar métricas para la valoración de las amenazas; iii) Diseñar métricas para la valoración de activos de información en base a criterios de riesgo; iv) Diseñar métricas para la valoración de controles de seguridad en base a estándares existentes y para calcular la probabilidad de ocurrencia de una vulnerabilidad.

Metodología - MARISMA.M

La tercera parte del marco de trabajo que estamos desarrollando contiene la metodología que se aplicará para la tasación objetiva de un sistema de información y la generación de un análisis de riesgo objetivo que tenga en cuenta aspectos asociativos y jerárquicos, reutilización del conocimiento, dinamismo, y que sea válida para las PYMES.

La metodología MARISMA está constituida por los siguientes artefactos:

- *Sistema de Tasación de Activos (STA)*: Permite, a partir de la lista de activos de la compañía, obtener una tasación económica de los mismos. Esta tasación se realizará en base a criterios totalmente objetivos, de forma que el valor de los activos no varíe si dos consultores diferentes realizan la tasación sobre los mismos activos. La tasación tendrá en cuenta también que pueden actuar sobre el valor de un activo dos tipos de factores: i) Factores jerárquicos: Por ejemplo, en el caso de una empresa filial, es posible que un determinado activo no le pertenezca, sino que sea propiedad de la matriz. O que la matriz deje ese activo a la filial mediante un leasing, con lo que sólo poseerá un porcentaje del activo; ii) Factores asociativos: Por ejemplo, un producto del cual la compañía se encargue de desarrollar el software, siendo incorporado el hardware por otra compañía asociada. En este caso, el valor del producto tasable para la compañía será sólo el correspondiente a la parte software del mismo. Este proceso está formado por cinco tareas: T1 – Lista de activos de la compañía; T2 – Rellenar el conjunto de propiedades de los activos; T3 – Calcular el valor total del activo; T4 – Aplicar factores asociativos y jerárquicos; T5 – Calcular el valor del activo en la compañía.
- *Sistema de Valoración Objetivo de Amenazas (SVOA)*: Permite valorar en base a métricas objetivas la probabilidad de ocurrencia de cada posible amenaza que puede afectar a cada uno de los activos de la compañía. En este sistema será básica la Base de Conocimiento que se va alimentando de cada nueva implantación, de forma que se pueda calcular automáticamente la probabilidad de ocurrencia de una amenaza en función de la calculada previamente para otra compañía con similares características. Por ejemplo, en función del ámbito geográfico. Los valores calculados también se verán afectados por la aplicación de factores jerárquicos y asociativos. Este proceso está formado por tres tareas: T1 – Pedir características de la compañía; T2 – Pedir factores asociativos y jerárquicos; T3 – Calcular el nivel de amenaza de la compañía.
- *Sistema de Medición Objetiva de Vulnerabilidades (SMOV)*: Permite valorar mediante métricas objetivas la probabilidad de que una vulnerabilidad pueda ser explotada para una compañía. Este sistema trabaja como parte fundamental una ontología de vulnerabilidades, para cada una de las cuales se calculará la probabilidad de ocurrencia. Este valor se calculará en función del los niveles de cobertura de los controles implantados en la compañía. De esta forma, el sistema trabajará sobre la base de un listado de controles. Para la primera

versión de la metodología se empleará el listado de controles de seguridad de la Norma ISO 27001 [10]. Los valores calculados también se verán afectados por la aplicación de factores jerárquicos y asociativos. Este proceso está formado por cinco tareas: T1 – Calcular el nivel de cobertura de los controles; T2 – Lista de vulnerabilidades; T3 – Probabilidad de ocurrencia de la vulnerabilidad; T4 – Aplicar factores asociativos y jerárquicos; T5 – Calcular el valor del activo en la compañía.

- *Sistema de Valoración de Activos Objetivo (SVAO)*: Permite dar un valor, de forma cuantitativa y objetiva, a cada uno de los activos de la compañía sobre la base de los principales criterios de riesgo (Confidencialidad, Integridad, Disponibilidad y Legalidad). Para ello se emplearán métricas que tomen como base estos criterios de riesgo. Los valores calculados también se verán afectados por la aplicación de factores jerárquicos y asociativos. Este proceso está formado por cinco tareas: T1 – Lista de activos de la compañía; T2 – Rellenar el conjunto de propiedades de los activos; T3 – Calcular el valor total del activo; T4 – Aplicar factores asociativos y jerárquicos; T5 – Calcular el valor del activo en la compañía.

En función de las valoraciones obtenidas por los sistemas SMOV (Probabilidad de ocurrencia de vulnerabilidades) y SVAO (Valoración de activos en base a criterios de riesgo), podemos obtener un valor de riesgo objetivo para cada uno de los activos de la compañía. Para realizar esto, nos estamos basando en las investigaciones de Feng [25] sobre generalización de la teoría Bayesiana de probabilidad subjetiva, las del modelo híbrido (probabilístico y posibilístico) de Carlsson [26], y métodos de inferencia difusa (fuzzy inference) para desarrollar modelos inteligentes de evaluación de riesgos en línea (intelligent online risk assessment models) propuestos por Abraham [27], entre otras [28]–[36]. Todas ellas orientadas a disminuir el grado de incertidumbre en la generación del análisis de riesgos.

Una vez calculado un valor de riesgo objetivo para cada activo, se podría utilizar como base para el cálculo del seguro del Sistema de Información de la compañía, ya que contamos también con la valoración económica objetiva de cada activo calculada previamente en el sistema STA. Como comentamos anteriormente, para la valoración económica de los activos nos estamos basando en las investigaciones de Lambrinoudakis [13].

Como hemos visto, los factores jerárquicos y asociativos se aplican a todos y cada uno de los sistemas que conforman el núcleo de la metodología. Asimismo, para el diseño y aplicación de la misma es necesario contar con una tercer factor: La necesidad de que la metodología sea dinámica, de forma que si hay algún cambio en el sistema (Por ejemplo, añadir un nuevo activo o un control que originalmente no se aplicaba) se puedan recalcular los valores de riesgo y tasación de una forma automática y ágil. Para definir estos aspectos nos estamos basando en las investigaciones de [26], [32], [37]–[39].

IV. Conclusiones y trabajo futuro

En este trabajo se ha propuesto MARISMA, un marco de trabajo que permite la tasación objetiva de un sistema de información y la generación de un análisis de riesgos objetivo que tenga en cuenta aspectos asociativos y jerárquicos y sea de bajo coste en su generación y mantenimiento.

Durante la investigación, se han estudiado las principales metodologías existentes en el mercado relacionadas con la generación de análisis de riesgos y se ha realizado una revisión sistemática de los diferentes modelos y metodologías para el análisis y gestión de riesgos, con el objetivo de estudiar las propuestas centradas en riesgos asociativos y jerárquicos orientadas a PYMES.

Como resultado de esta revisión se ha podido establecer la importancia que tiene la gestión y el análisis de los riesgos sobre la seguridad de los Sistemas de Información en el desempeño y evolución sostenible de las empresas, ya que constituye un requisito básico para alcanzar la misión y los objetivos organizacionales en un entorno altamente competitivo.

Además, se han realizado reuniones y entrevistas en empresas privadas y sectores como el asegurador, para establecer las necesidades reales de las empresas y terceros, de forma que la investigación tenga una clara aplicación práctica.

Se ha podido validar durante la investigación la problemática de aplicar las metodologías existentes en el caso de las PYMES, ya que éstas han sido concebidas para grandes empresas, siendo la aplicación de este tipo de metodologías y modelos difícil y costosa para las PYMES [40]–[44].

El problema principal de todos los modelos de análisis y gestión de riesgos existentes es que no están teniendo éxito a la hora de implantarse en PYMES, debido principalmente a que:

- Unos fueron desarrollados pensando en organizaciones grandes (Grandes estándares como CRAMM [23], ISO/IEC 27005 [17], MAGERIT [20], OCTAVE [45], NIST SP 800-39 [46], MEHARI [21] o COBIT [47]) y en las estructuras organizativas asociadas a éstas.
- Otros [37], [39], [48] han intentando simplificar el modelo para que pudiera ser apto para compañías con recursos limitados, pero son modelos incompletos que sólo afrontan parte del problema, o intentan aportar unas guías básicas de los pasos a realizar, pero sin entrar en cómo evaluar y gestionar realmente los riesgos de una forma en la que el propio personal técnico de la empresa se pueda involucrar. Además, la mayoría son modelos teóricos y están todavía en desarrollo.
- La mayoría de las propuestas no tienen en cuenta la necesidad de contemplar riesgos jerárquicos y asociativos, factores cruciales en la estructura y funcionamiento actual de las empresas (en el que cada vez tiene más peso el uso de sistemas en Cloud), sobre todo de las PYMES.
- No existen formas objetivas de realizar un análisis de riesgo, dejando gran parte de la responsabilidad a los consultores, de forma que los resultados no tienen validez para terceros.

- La valoración económica de los activos de información es subjetiva, al no existir formas objetivas de valorarlo.

De esta forma, creemos que la investigación propuesta es el inicio de una propuesta detallada y ambiciosa, ya que solucionará gran parte de la problemática existente con las metodologías actuales y tendrá una clara aplicación práctica.

Las ventajas de la investigación propuesta son claras; la posibilidad de poder tener mecanismos de tasación de sistemas de información y de análisis de riesgos que sean objetivos, con coste reducidos y que tengan en cuenta las interrelaciones de los activos supone un cambio radical en la forma de ver los análisis de riesgo, ya que estos se convierten en herramientas útiles para los terceros (ej: las aseguradoras) y posibilita que las compañías tengan mecanismos objetivos de comparación de los riesgos cuando contratan un proyecto a otra compañías.

Todos los estándares y propuestas para la evaluación y gestión de riesgos estudiados en este trabajo son muy importantes, y sus aportaciones serán tenidas en cuenta para el desarrollo de una metodología que incluya todas las características deseadas.

Agradecimientos

Esta investigación es parte del proyecto PROMETEO financiado por la Secretaría Nacional de Educación Superior, Ciencia, Tecnología e Innovación (SENESCYT) del Gobierno de Ecuador, y el proyecto SIGMA-CC (Ministerio de Economía y Competitividad y el Fondo Europeo de Desarrollo Regional FEDER, TIN2012-36904).

Referencias

[1] Kluge, D. Formal Information Security Standards in German Medium Enterprises. in CONISAR: The Conference on Information Systems Applied Research. 2008.

[2] Dhillon, G. and J. Backhouse, Information System Security Management in the New Millennium. Communications of the ACM, 2000. 43(7): p. 125-128.

[3] Barlette, Y. and V. Vladislav. Exploring the Suitability of IS Security Management Standards for SMEs. in Hawaii International Conference on System Sciences, Proceedings of the 41st Annual. 2008. Waikoloa, HI, USA.

[4] Wiander, T. and J. Holappa, Theoretical Framework of ISO 17799 Compliant. Information Security Management System Using Novel ASD Method., in Technical Report, V.T.R.C.o. Finland, Editor 2006.

[5] Wiander, T. Implementing the ISO/IEC 17799 standard in practice - experiences on audit phases. in AISC '08: Proceedings of the sixth Australasian conference on Information security. 2008. Wollongong, Australia.

[6] Michalson, L., Information security and the law: threats and how to manage them. Convergence, 2003. 4(3): p. 34-38.

[7] Volonino, L. and S. Robinson. Principles and Practice of Information Security. in 1 edition, Anderson, Natalie E. 2004. New Jersey, EEUU.

[8] Spinellis, D. and D. Gritzalis. nformation Security Best Practise Dissemination: The ISA-EUNET Approach. in WISE 1:First World Conference on Information Security Education. 1999.

[9] A., S.-O., et al. Revisión Sistemática de Metodologías y Modelos para el Análisis y Gestión de Riesgos Asociativos y Jerárquicos para PYMES. in XII Reunión Española sobre Criptología y Seguridad de la Información (RECSI12). 2012. Donostia, San Sebastián (España): Septiembre, 2012.

[10] ISO/IEC27001, ISO/IEC 27001, Information Technology - Security Techniques Information security management systemys - Requirements., 2013.

[11] Alhawari, S., et al., Knowledge-Based Risk Management framework for Information Technology project. International Journal of Information Management, 2012. 32(1): p. 50-65.

[12] Hewett, R. and R. Seker, A Risk Assessment Model of Embedded Software Systems. 29th Annual IEEE/NASA Software Engineering Workshop (SEW'05), 2005: p. 8.

[13] Lambrinoudakis, C., et al., A formal model for pricing information systems insurance contracts. Computer Standards amp; Interfaces, 2005. 27(5): p. 521-532.

[14] Stewart, T.A., Trying to grasp the intangible. Fortune, 1995: p. 91.

[15] ISO/IEC13335, ISO/IEC 13335, Information Technology - Security Techniques - Management of Information and Communications Technology Security, 2004.

[16] ISO/IEC27002, ISO/IEC 27002:2005, the international standard Code of Practice for Information Security Management (en desarrollo). 2007.

[17] ISO/IEC27005, ISO/IEC 27005. Information Technology - Security Techniques - Information Security Risk Management Standard, 2008.

[18] Stoneburner, G., A. Goguen, and A. Feringa. Risk Management Guide for Information Technology Systems, NIST SP 800-30. 2009.

[19] 4360:2004, A.N., Standars Australia and Standards New Zealand. Risk Management2004, Sydney, NSW.

[20] MageritV2, Methodology for Information Systems Risk Analysis and Management (MAGERIT version 2), 2006, Ministerio de Administraciones Públicas (Spain).

[21] MEHARI. Club de la Sécurité de l'Information Français. 2009; Available from: https://www.clusif.asso.fr/.

[22] OCTAVE. CERT - Software Engineering Institute, Carnegie Mellon. 2009; Available from: http://www.cert.org/octave/.

[23] CRAMM. Siemens Enterprise Communications Ltd. ÇRAMM toolkit". 2009; Available from: http://www.cramm.com/.

[24] [24]ISO/IEC27002, ISO/IEC 27002, Information Technology - Security Techniques - The international standard Code of Practice for Information Security Management., 2013.

[25] Feng, N. and M. Li, An information systems security risk assessment model under uncertain environment. Applied Soft Computing, 2011. 11(7): p. 4332-4340.

[26] Carlsson, C. and R. Fullér, Predictive Probabilistic and Possibilistic Models Used for Risk Assessment of SLAs in Grid Computing. IPMU 2010, Part II, CCIS 81, 2010: p. 747-757.

[27] Abraham, A., Nature Inspired Online Real Risk Assessment Models for Security Systems. EuroISI 2008, LNCS 5376, 2008.

[28] Chang, S.-I., et al., The development of audit detection risk assessment system: Using the fuzzy theory and audit risk model. Expert Systems with Applications, 2008. 35(3): p. 1053-1067.

[29] Wang, P., et al., A Fuzzy Decision Model of Risk Assessment Through Fuzzy Preference Relations with Users'Confidence-interval. IEEE Computer Society AINA'06, 2006.

[30] Deng, Y., et al., Risk analysis in a linguistic environment: A fuzzy evidential reasoning-based approach. Expert Systems with Applications, 2011. 38(12): p. 15438-15446.

[31] Ngai, E.W.T. and F.K.T. Wat, Fuzzy decision support system for risk analysis in e-commerce development. Decision Support Systems, 2005. 40(2): p. 235-255.

[32] Kumar, V., M. Schuhmacher, and M. García, Integrated Fuzzy Approach for System Modeling and Risk Assessment. MDAI 2006, LNAI 3885, 2006: p. 227 - 238.

[33] Lin, M., Q. Wang, and J. Li, Methodology of Quantitative Risk Assessment for Information System Security. CIS 2005, Part II, LNAI 3802, 2005: p. 526 - 531.

[34] Lo, C.-C. and W.-J. Chen, A hybrid information security risk assessment procedure considering interdependences between controls. Expert Systems with Applications, 2012. 39(1): p. 247-257.

[35] Patel, S.C., J.H. Graham, and P.A.S. Ralston, Quantitatively assessing the vulnerability of critical information systems: A new method for evaluating security enhancements. International Journal of Information Management, 2008. 28(6): p. 483-491.

[36] Salmeron, J.L. and C. Lopez, A multicriteria approach for risks assessment in ERP maintenance. Journal of Systems and Software, 2010. 83(10): p. 1941-1953.

[37] Nachtigal, S., E-business Information Systems Security Design Paradigm and Model. Royal Holloway, University of London, Technical Report, 2009: p. 347.

[38] Arikan, A.E., Development of a risk management decision support system for international construction projects. Middle East Technical University, 2005: p. 118.

[39] Ma, W.-M., Study on Architecture-Oriented Information Security Risk Assessment Model. ICCCI 2010, Part III, LNAI 6423, 2010: p. 18-226.

[40] Batista, J. and A. Figueiredo, SPI in very small team: a case with CMM. Software Process Improvement and Practice, 2000. 5(4): p. 243-250.
[41] Hareton, L. and Y. Terence, A Process Framework for Small Projects. Software Process Improvement and Practice, 2001. 6: p. 67-83.
[42] Calvo-Manzano, J.A., et al., Experiences in the Application of Software Process Improvement in SMES. Software Quality Journal., 2004. 10(3): p. 261-273.
[43] Tuffley, A., B. Grove, and M. G., SPICE For Small Organisations. Software Process Improvement and Practice, 2004. 9: p. 23-31.
[44] Mekelburg, D., Sustaining Best Practices: How Real-World Software Organizations Improve Quality Processes. Software Quality Professional, 2005. 7(3): p. 4-13.
[45] Alberts, C.J. and A.J. Dorofee, OCTAVE Criteria, Version 2.0, 2001.
[46] NIST, Security Metrics Guide for Information Technology Systems, 2004.
[47] COBITv4.0, Cobit Guidelines, Information Security Audit and Control Association, 2006.
[48] Abdullah, H., A Risk Analysis and Risk Management Methodology for Mitigating Wireless Local Area Networks Intrusion Security Risks. University of Pretoria, 2006: p. 219.