Information Security Measurement Infrastructure for KPI Visualization

Kemal Hajdarevic*, Colin Pattinson**, Kemal Kozaric***, Amela Hadzic****
*Faculty of Electrical Engineering, University of Sarajevo, Sarajevo, Bosnia and Herzegovina
**Faculty of Art, Environment and Technology, Leeds Metropolitan University, Leeds, UK
***Central Bank of Bosnia and Herzegovina, Sarajevo, Bosnia and Herzegovina
****BH Telecom, Sarajevo, Bosnia and Herzegovina

E-mail(s):KHajdarevic@etf.unsa.ba, C.Pattinson@leedsmet.ac.uk, KKozaric@cbbh.ba, Amela.Hadzic@bhtelecom.ba

Abstract – In last decade information security standards became well documented starting with ISO 27001:2005 which defines requirements for a organisation's Information Security Management System (ISMS). Other standards such as ISO 27004:2009, 27003, and 27005 are published later too. Organisational ISMS can be certifies for ISO 27001:2005 certificate and it adopts Plan-Do-Check-Act (PDCA) life cycle of constant system improvements. To be able to improve operations and information security ISO 27004:2009 standard has to be used to create useful Key Performance Indicators (KPI) in order to achieve constant improvements of the ISMS. During phase of maintenance every system needs infrastructure to collect data, analyse data and then to create KPI for constant improvements. In this paper is presented information security measurement infrastructure for KPI visualisation based on practical experience from production system in financial surrounding.

I. INTRODUCTION

For every business it is important to secure their operations and manage information security risk by using available data to create information and analyse that information to acquire new knowledge and improve operations. Probably the easiest way is to do it, is to use already available standardized methods such as implementing information security standards in order to manage information security risk. To manage Information security risk in terms of ISO 27001:2005 [1, 14, 15] standard is to manage risk connected to vulnerabilities and associated threats and impacts on Confidentiality, Integrity and Availability (CIA) of organisation or company information assets. Information assets are usually classified as: people, services, hardware, software, intangibles, utilities [1]. Information security is important for every person and organisation because today there are many activities which involve usage of secret or private information. For persons that might be social ID, PIN number for credit and mobile phone SIM cards, or personal biometric information such as fingerprint or retina readings, and even personal dairy. On the other hand, for any organisation or company all data related to a particular person mentioned above, and for all data and other organisation's or information assets CIA has to be provided there where it is necessary. To be able to provide reasonable assurance that risk management is working and that system is improved in every PDCA cycle, Key Performance Indicators (KPI) have to be collected and presented for making meaningful decisions. Here KPI represent information (similar to car dashboard with speed meter) which are used to make decisions that will correct future actions what can be used to accomplish specific goal. KPI might be compared to autopilot of organisation which responsible to keep business activities on right path.

Presentation of specific KPI is a result of information security measurement process [17, 18, 19, 20]. Organisation's information security goals and objectives can be reached with appropriate decisions created using exact system information by constant monitoring and measuring system KPIs [21, 22,]. Information security measurements are used to make easier process of making decisions helping in better accountability and performance management by collecting, analysing and reporting relevant KPIs [2]. The main reason to monitor KPIs is to provide information of status for specific activity or monitored process which will be used for improvements of those activities related to information security by implementing corrective and preventive actions based on objective results of measurements as it is presented in literature [16, 23, 24].

As it is already announced in abstract, below is presented holistic approach for data collection, data mining and KPI visualisation, rather then presenting only one aspect of measuring and managing performance and compatibility with information security standard such as 27001:2005 [1]. All results and proposals are done as a result of more than five years (preparation, implementation, and maintenance) of practical experience (of authors referenced above - Governor[3] member of Security Forum of Central Bank of Bosnia and Herzegovina (CBBH) and Information

Security Manager[1]) from Information Security Management System (ISMS) of CBBH which is certified for ISO 27001:2005 by authorised certification authority, started in 2009. In the specific ISMS implementation presented in this paper is used name of the organisational body role called Security Forum which represents top management responsible for making strategic decisions. Second important role is Information Security Manager which is responsible to coordinate and report all information security related activities and acts as information / action bus between Security Forum and organisation departments, divisions and sections and external / internal auditors. Practical experience from the real system could help for better understanding real situation and could help in developing better simulation tools for different business surroundings. Simulation tool for industrial surrounding such as power plant infrastructure is presented in the paper [8] for simulating security assessment of computer and network infrastructure targeted by malware attacks. This approach [8] is good to test potential risk and impacts in specific situations such as malicious – malware attacks, where specific and relevant data can be better recognized which will, be used as data for metrics and creation of useful KPIs.

II. Architecture Model for Data Collection, Calculation, Combination and KPI Visualisation

We grouped all ISO 27001:2005 controls in five groups related to area of application starting from number 2 (shown in Figure 3. Below) to Physical and Technical Security(2), IT or logical security (3), Common Affairs Security (4), Human Resources Security(5), and Legal Security (6). Presented grouping was done based on conducted risk assessment process and GAP analysis. Architecture model for data collection, combination and visualisation presented in Figure 3. is based on model [12] already used for Service Oriented Architecture (SOA) business model. In architecture model presented here are incorporated enhancements and customisation for ISMS managing purposes. This model proposes central point of data collection from five presented areas of information security.

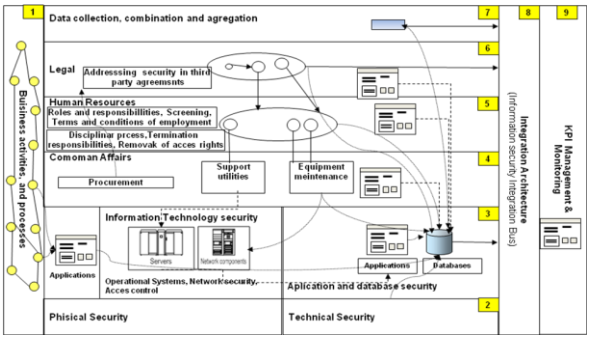


Figure 3. ISMS Architecture model based on [12]

III. Infrastructure for Data Collection, Calculation, Combination and KPI Visualisation

As a sample, for data collection point was used incident management system for reporting information security incidents.

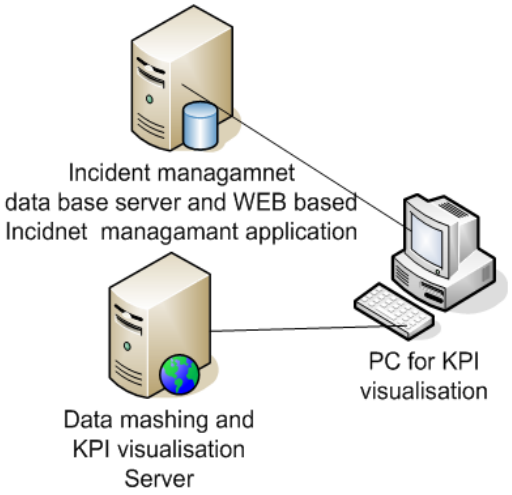


Figure 1. Infrastructure for data collection and KPI visualisation

These incidents are related to hardware and software information assets such as virus occurrences as result of removable media usage, Internet site browsing etc. General security incidents other than related to hardware and software are reported on incident management system. All data are stored in Microsoft SQL database.

In this database are created tables which contains data such as type of incident, location of incident, time of incident, time when incident is resolved, name of person who resolve and incident, source of infection and other relevant data. For the testing purposes was used ARIS MashZone software [10] able to read data and visualized them.

IV. Choosing Relevant Data for KPI Metrics

In order to successfully and constantly improve (PDCA) information security of the organization or company it is necessary to chose right processes, activities, and metrics to measure. There are number of ways which was used in past in order to standardize security metrics and measurement processes such as [4] and to propose research directions directions in security metrics [5]. One method which is accepted as the standard is ISO 27004:2009 [6] or NIST guide [2] for determining meaningful KPIs. This standard [6] provides guidance how to produce effective measurements and it gives examples in documented standard appendices how to create metrics for specific controls and how to measure results for specific controls from ISO 27001:2005[1]. Written sources

such as [7] provide details on how to measure effectiveness of security control implementations for managing application design, application implementation and their maintenance. Relevant data can be obtained and collected at different levels of organisation and can be used together, aggregated and rolled up to the higher levels of the organisation to create appropriate reports.

V. Relevant Data Collection Process

The most suitable way to collect relevant data is to automate this process where metrics have to be presented as number or percentage to present more objective results [7]. As an example of ISO 27001:2005 [1] metric for control *10.1.4* with the title "*Separation of development, test and operational facilities"* is percentage of critical applications that have a separate test environment. Using this simple but effective metric it is possible in objective way asses current risk that critical applications do not have surrounding for testing purposes. Critical application without test environment could create risk to test new system features on production system what can create unpredictable production system behavior.

VI. Data Calculation Formulas

We are not aware that it is already presented architecture model and infrastructure for data collection, data mining and presentation KPIs in intuitive and easy way as we trying to propose in this paper. In this paper is presented architecture and infrastructure to collect data, data mining and as a result to present KPIs in easy and meaningful way ready to be used for decision making.

We decided to present two examples with complete cycle of data collection and data mining for ISO 27001:2005 controls *7.1.3 Acceptable usage of assets* (MA713) and *10.4.1 Protection against malicious code*.

To decide how KPIs have to be created ISO 27001:2005 [1], 27004:2009 [6], [7] were used and risks assessment was performed. As a result for the control *7.1.3 Acceptable usage of assets* is chosen number of security malware incidents (MIN) occurred as a result of unacceptable way of assets usage such as bringing infected removable media (MIRM) with malware or browsing malware infected Internet sites (MIS). And having current system information it is set below acceptable values or goals where:

$$MIN = MIRM + MIS$$

MA713 = MIN <10 acceptable; MIN <10 not acceptable

And for the control *10.4.1 Protection against malicious code* (MA1041) is used ratio of malware incidents number (MIN) of recognised by internal protection system (anti-virus software) and malwares stopped (MS) at the system gate using following formula:

$$MA1041 = (MIN/MS)*100$$

MA1041 ≤ 0,1 acceptable; MA1041> 0,1 not acceptable

In similar way it is possible to initiate data collection for any other control. It is necessary for data collection that data are stored in one or more databases or tables so that they can be used for data mining and producing reports.

VII. Data Operations - Feeds, Calculations and Mashing Data

Recent research results show how [9] data presentation might be hard to monitor and manage since human information security manager might be overwhelmed with level of information that system produce shown in Figure 2 [9].

This is important since decision makers for information security are usually members of top management (Security Forum) which do not want large quantity of information to handle because it can prolong time for making decisions. It is to management decision to allow new funding or resources to support implementation of new controls, proposed in preventive and corrective actions as result of monitoring KPIs. Instead of having more levels of reporting [9] as it is shown in Figure 2. see below, where 8 levels of reporting is shown (details in Figure 2. are not important for this purpose which can be find in referenced paper but level of reporting), in this paper is proposed two level reporting approach.

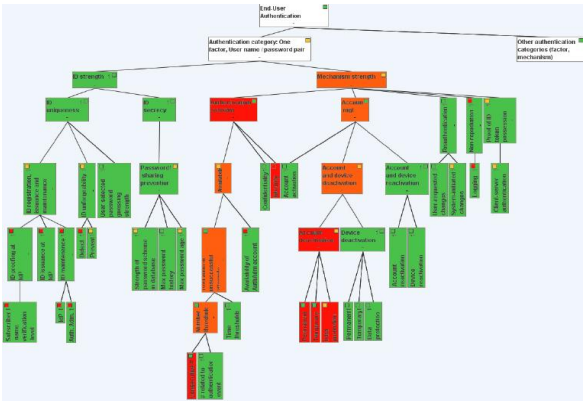


Figure 2. Visualisation Tool [9]

First level, or highest level of reporting where it is reported if control satisfies desired goals or not is intended for reporting top management (Security Forum).

Second level of reporting gives more details where reasons of specific problems can be marked and find reasons for not complying with goals previously set. This level of reporting is intended for Information

Security Manager and is used for making proposals for corrective and preventive actions in order to propose them to top management – Security Forum.
Commercial software such as ARIS MashZone [10] can be used search through data (data mining) and interpret KPIs by feeding data from databases such as Microsoft, Oracle, or Excel, CSV, or XML files, HTML web sites, or it can allows manual data feeds. ARIS MashZone [10] is primarily intended to be used for generic process monitoring and KPI management. By meshing data (meshing here means: to use data from different sources by combing, converting them, and to perform other operation to extract useful data) from different sources (databases, files and manual entries) it is possible to discovery knowledge not only from data bases, but from other sources too, especially by combining different sources together. Above presented solution for searching knowledge allows to read specific columns from tables of different sources. Different operation can be done with data from columns such as calculation (aggregation, arithmetic, average, round, etc.), change data type, insert, duplicate, delete, rename, manage different operations with date and time and other possibilities too.

For the presented control *7.1.3 Acceptable usage of assets* (MA713) in section *6. Data collection formulas* are taken columns which contains data: occurrence of the event, type of event (MIRM and MIS – see section *6. Data collection formulas*), time of finishing report for each event, open or closed status for each report of event which is monitored dynamically through the time having (see section *6. Data collection formulas*):

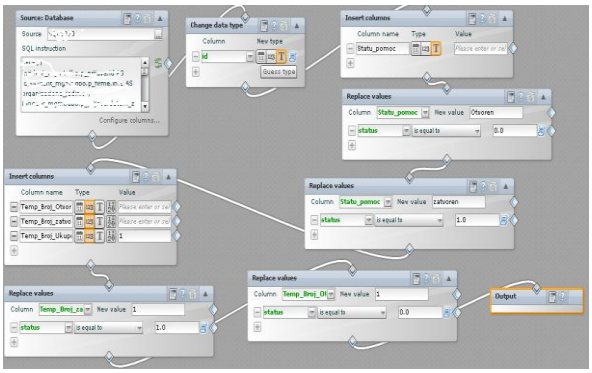
$$MIN = MIRM + MIS$$

For the presented *10.4.1 Protection against malicious code* (MA1041) in section 4, Data collection - are taken columns from tables from different Excel files. These files contains data: number of stopped viruses and trojans on network gates with Internet and value of MIN from control *7.1.3 Acceptable usage of assets* (MA713) to be used in this relation:

$$MA1041 = (MIN/MS)*100$$

Below in Figure 2. - Mashup data feeds is shown one mashup (here mashup means representation of relations and operation on data taken from different data sources) screen shot. In this mashup are incorporated above formulas which create results in two-dimensional table. This table is ready to be used for data filtering and presentation – visualisation.

This approach to collect data from different sources allows infrastructure to combine, and aggregate data from different levels of organisation and to create joint reports.



3. Mashup data feeds

VIII. KPI VISUALISATION

Purpose for all data collection and later for data mining is to visualize KPI results in time window. For testing KPI visualisation purposes was used ARIS MashZone [10] software.

According to specific time frames for PDCA cycles specific time window resolution can be chosen such as Yearly, Quarterly, Monthly, weekly, daily, or other KPI result representation for all or specific categories.

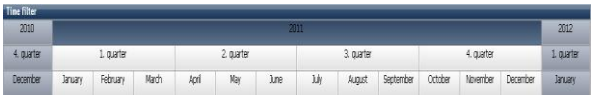


Figure 4. Yearly, Quarterly, monthly data

Top infected units, with names of responsible employees, locations of misused computer equipment, and other information assets.

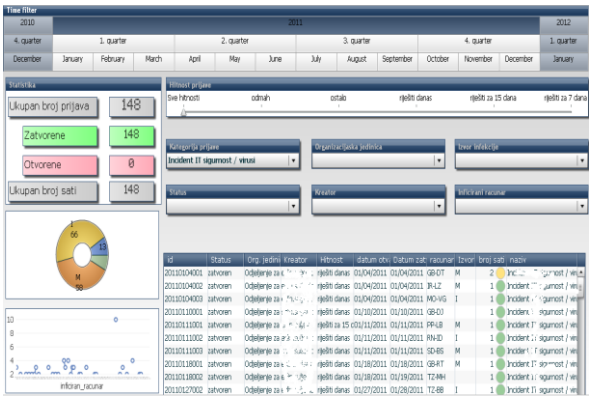


Figure 5. KPI visualisation window

By visualising and tracing KPI through the time is possible to adjust metric settings for tracking specific problems and avoid their future and possible occurrences. Process of information security improvements starting with base measurement

performed and by implementing corrective and preventive actions and monitoring trends and their effects with goal to reduce information security risk on information assets.

IX. CONCLUSIONS

While in other papers and documents [7], [8], [9] are presented partial solutions to crate and monitor information security KPIs, in this paper is presented architecture and infrastructure for whole solution for data collection, mining and KPI presentation. For monitoring information security KPIs in production or research environment infrastructure environment is needed to collect and present data. Presented environment might seems as already seen but presented approach show experienced knowledge and building blocks for researchers which would like to establish their own infrastructure environment for KPI visualisation. Best research results and experience could come from real world situations generated on production systems.

Reports and KPIs can be created with open source tools such as ReportManager [11] not only with commercial software like MashZone [10] used here only for test purposes, or HP Executive scorecard. Other available commercial solutions offer holistic solutions for data collection, mining and reporting too.

REFERENCES

[1] Information Technology – Security techniques – Information security management – Requirements, ISO / IEC 27001:2005, 31.6.2004 First edition.

[2] Chew E., Swanson M., Stine K., Bartol N., Brown A., and Robinson W., Performance Measurement Guide for Information Security. NIST, July 2008, Available at: http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf, [Acessed on: 25.1.2012]

[3] Calder A. and Watkins S.G, Information Security Risk Management for ISO27001 / ISO17799, pp 91. IT Governance Publishing 2007. ISBN 978-1-905356-23-2.

[4] Pazne C. Shirley, A Guide to Security Metrics, SANS Institute, 19 June, 2006. Available at: http://www.sans.org/reading_room/white papaers/auditing/guide-security-metrics_55 [Accessed on: 10.1.2012]

[5] Jansen W., Directions in Security Metrics Research, National Institute of Standards and Technology, US Department of Commerce. NISTR 7564. April 2009.

[6] Information Technology – Security techniques – Information security management – Measurement, ISO / IEC 27004:2009, 15.12.2009 First edition.

[7] Vasudaven V, Mangla A, Ummer F. Shetty S. Pakala S. Anbalahan S. Aplication Security in the ISO27001 Environment, 2008. Governance Publishing. ISBN 978-1-905356-35-5.

[8] R. Leszczyna I.N., Fovino M., Masera, Approach to security assessment of critical infrastructures' information systems. Published in IEEE, IET Information Security, Volume 5, Issue:3, pages 135-144, Issue date September 2011.

[9] Savola R. M. Heinonen P.A, Visualisation and Modeling Tool for Security Metrics and Measurements Management. Information Security South Africa (ISSA) 2011 IEEE, ISBN 978-1-4577-1481-8.

[10] MashZone Available at: www.mashzone.com [Accessed on: 10.1.2012]

[11] Report Manager, Available at: http://reportman.sourceforge.net [Accessed on: 10.1.2012]

[12] Karin Duremeyer, Methodology: From Component Business Model to Service Oriented Architecture, 7.5.2004, IBM, Available at: http://www.minet.uni-jena.de/dbis/veranstaltungen/datenbanktage-2004/Doblaski,%20Lutz.ppt [Accessed on: 10.1.2012]

[13] HP Executive Scorecard, Available at: https://h10078.www1.hp.com/cda/hpms/display/main/hpms_content.jsp?zn=bto&cp=1-11-16-18%5E45777_4000_311__ , [Accessed on: 10.1.2012]

[14] Alan Calder, Implementing Information Security Based on ISO 27001/ISO 27002: A Management Guide, 2nd Edition (Best Practice (Van Haren Publishing)), 31 July 2009

[15] ISO/IEC 27004:2009 Information technology — Security techniques — Information security management - Measurement, Available at: dhttp://www.iso27001security.com/html/27004.html, [Accessed on: 14.3.2012]

[16] Rathbun D., Gathering Security Metrics and Reaping the Rewards, Octobar 2009, Available at: http://www.sans.org/reading_room/whitepapers/leadership/gathering-security-metrics-reaping-rewards_33234 [Accessed on: 14.3.2012]

[17] Brotby, W. K. (2009). Information security management metrics: a definitive guide to

effective security monitoring and measurement. Boca Raton, FL: Taylor & Francis Group, LLC.

[18] Center For Internet Security Security Metrics. (n.d.). Retrieved October 10, 2009, from Center For Internet Security: http://www.cisecurity.org/securitymetrics.html [Accessed on: 2.3.2012]

[19] Elizabeth Chew, M. S. (2008, July). NIST Special Publication 80055 Revision 1. Retrieved from NIST Computer Security Resource Center: http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf [Accessed on: 1.3.2012]

[20] Herrmann, D. S. (2007). Complete guide to security and privacy metrics: Measuring regulatory compliance, operational resiliance, and ROI. Boca Raton, FL: Auerbach Publications.

[21] Introduction To ISO 27004 Information Security Management, Measurement And Metrics. (n.d.). Retrieved October 10, 2009, from The ISO 27000 Directory: http://www.27000.org/iso-27004.htm [Accessed on: 11.3.2012]

[22] Jaquith, A. (2007). Security metrics: replacing fear, uncertainty, and doubt. Upper Saddle River, NJ: Pearson Education, Inc.

[23] SecurityMetrics.org (n.d.). Retrieved October 26, 2009, from securitymetrics.org: http://www.securitymetrics.org [Accessed on: 8.3.2012]

[24] Security Metrics: OnDemand (n.d.). Retrieved November 04, 2009, from metricscenter.net: https://www.metricscenter.net/ [Accessed on: 9.3.2012]