Journal of Central Banking Theory and Practice, 2012, 2, pp. 5-17 *UDC: 336.71*
Received: 14 May 2012; accepted: 11 June 2012.

***Kemal Hajdarevic*[*], *Kemal Kozaric*[**], *Jasmin Hadzigrahic*[***]**

[*] Information Security Manager, Governor's office, Central Bank of Bosnia and Herzegovina

E-mail: khajdarevic@ cbbh.ba

[**] Governor of the Central Bank of Bosnia and Herzegovina and a professor at the Faculty of Economics in Sarajevo.

E-mail: kkozaric@cbbh.ba

[***]Senior Specialist for Applications Design and Maintenance, IT Department, Central Bank of Bosnia and Herzegovina

E-mail: jhadzigrahic@cbbh.ba

Architecture and infrastructure for governing information security in central banks

Abstract – Everyday news reports reveal incidents and even large-scale scandals in the business world related to improper information security handling. Despite available and existing relevant information security standards, incidents which could lead to real problems were not proactively prevented for numerous of reasons. One of the first and most important reasons was not implemented and observed relevant information security standards such as ISO 27001. This standard defines requirements for an organisation's Information Security Management System (ISMS). Implementation of the ISMS is only the tip of the iceberg in managing information security since all system parts have to be well monitored and adjusted to prevent or minimize security risks. This process of monitoring and upgrading takes most of the resources dedicated to every ISMS. Standard such as ISO 27004:2009 which defines what has to be monitored also belongs to ISO 2700 series of standards. The ISO 27004:2009 standard does not define how measurement has to be done by using a specific kind of architecture and infrastructure for the Key Performance Indicator (KPI) measurement and monitoring. In this paper is presented holistic approach for implementing architecture and infrastructure to collect, analyse, and present information security KPIs, in order to achieve constant improvements of the ISMS. The same approach could be used for other business activities as well in central banks or other organisations.

Key words: Information Security, KPI, measurement

JEL: O31

1. Introduction

In recent news reports such as Barclays LIBOR case (Watkins, 2012) and numerous others cases, where technical information and communication means (e-mails, SMS) are used in improper way, shows us that subjects (here subjects means persons) were not aware of information security importance and how to manage it in a proper way. Wide range of institutions involved in information security incidents witness that there is need for better governing of information security. Information used by many business activities has to be available, confidential, and with guaranteed integrity. International set of standards for managing information security, or Confidentiality, Integrity, and Availability (CIA) of information is ISO 27000. For the ISO 27001 which is one of the standards from ISO 27000 set it is possible to get certificate upon implementing and maintaining Information Security Management System (ISMS). Like other international standards, ISO 27001:2005 is based on Deming's (Moen R. & Norman C, 2009) Plan-Do-Check-Act approach for constant system improvements. Information security standard offers framework for implementing ISMS, and other standards from the ISO 27000 family are helping in ISMS operation and management. The main gain for management of any organisation which have implemented ISMS is the ability to manage information security risk. Standard for implementing information security risk management inside ISMS is ISO 27005:2008 standard. In terms of information security risk management within ISMS, this means to manage risk connected to vulnerabilities and associated threats and impacts on Confidentiality, Integrity and Availability (CIA) of organisation or company information assets. Information security risk management is done by evaluating vulnerabilities and associated threats and impacts on Confidentiality, Integrity and Availability (CIA) of organisation or company information assets which is usually classified by: people, services, hardware, software, intangibles, and utilities ISO 27001:2005 (2005).

In order to control the security of information assets and associated risks, appropriate controls have to be implemented, those controls referenced in appendix of ISO 27001:2005, (2005) standard and any additional controls which need is recognized in the risk management process. While only a limited set of Key Performance Indicators (KPI) data is available for the initial ISMS implementation, continuous monitoring of quality and performance execution of controls provides an opportunity to improve the system results. In information security, KPI is data which is used by the management for the purpose of informed decision-making by using relevant measured data. These KPI are usually presented in the form of trends or dashboards to make it easier for decision makers to identify the room for improvements. After more that five years of experience with

ISO 27001:2005 in the Central Bank of Bosnia and Herzegovina (CBBH) from the Information Security Management System (ISMS) of the CBBH which is certified for ISO 27001:2005 by authorised certification authority, which started in 2009 ans lasted until 2012, we became aware that there is a need for a systematic monitoring of relevant KPI. The only way to achieve this is by introducing a system for KPI visualisation (Hajdarevic et al, 2012). The system for KPI monitoring can be seen as an autopilot of specific organisation to be used to manage business activities in order to satisfy an organisation's strategic goals.

This paper illustrates the specific ISMS implementation of architecture and infrastructure as a support for the CBBH decision-making body called the Security Forum. The Security Forum is top management, responsible for making decisions regarding information security issues. Every ISMS has the Information Security Manager (IMS) responsible for coordination of information security activities, reporting all information security related incidents and acting as information/ action hub between the Security Forum and organisational departments, divisions and sections and external/internal auditors.

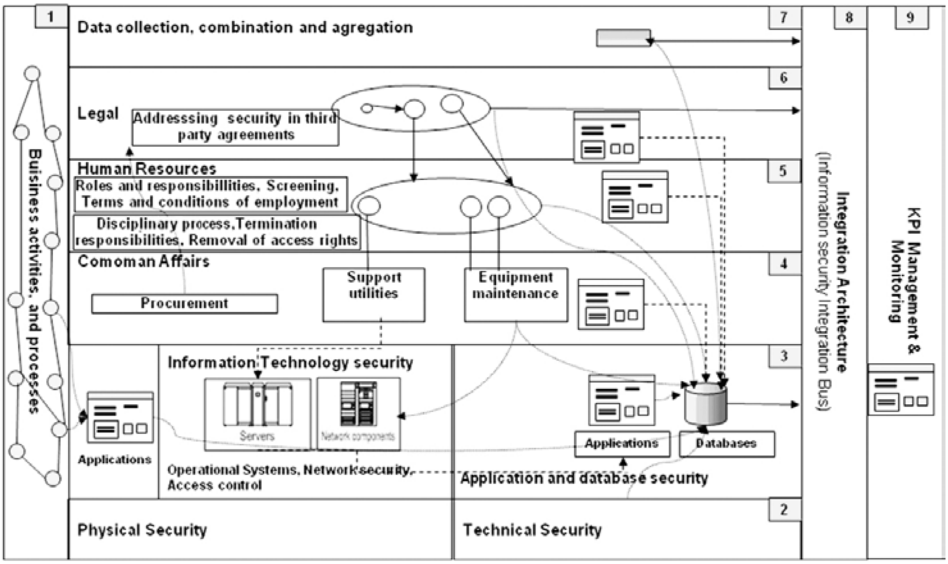
During the process of the ISMS implementation in the CBBH, we did not have time to prepare the system by using simulation tools as it is usually done, but instead we had to deal with real data and real situations because of the tight timeframe for the system to be put in operation. In later research we found it useful to use simulation tools for KPI visualisation such as tool (Leszczyna et al., 2011) used to simulate security assessment of computer and network infrastructure targeted by malware attacks. Simulation tools such as (R. Leszczyna et al, 2011) is good to test potential risks and impacts in specific situations, where specific and relevant data can be determined and analysed, then used as relevant data for creating appropriate KPI metrics for the decision-making process.

Simulation tools and practical experience from the real system, together can be used for a better understanding of production in different and real business environments.

2. Data collection architecture model for data collection, calculation, combination and KPI visualisation

We implemented all ISO 27001:2005 controls taking five major areas of business activities into account by grouping relevant controls to specific business activity as a major supporter for specific control. Figure 1 shows the architecture of data collection, calculation, combination and KPI visualisation related to the specific information security area of operation. Five areas of information security management shown in Figure 1 are presented in this model. Architecture model for data collection, combination and visualisation presented in Figure 1 (Hajdarevic et al, 2012) is based on the model (Duremeyer, 2004) already used for Service Oriented Architecture (SOA) business model.

Figure 1: ISMS Architecture model (Hajdarevic et al, 2012)


1
Data collection, combination and agregation
7
8
9
6
Legal
Addresssing security in third party agreements
Human Resources
Roles and responsibillities, Screening, Terms and conditions of employment
Disciplinary process,Termination responsibilities, Removal of access rights
5
Comoman Affairs
Procurement
Support utilities
Equipment maintenance
4
Buisiness activities, and processes
Integration Architecture
(Information security Integration Bus)
KPI Management & Monitoring
Information Technology security
3
Servers
Network components
Applications
Operational Systems, Network security, Access control
Applications
Databases
Application and database security
2
Physical Security
Technical Security

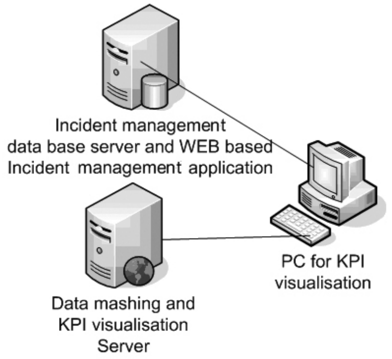
Five areas of information security shown in Figure 1 are: Physical and Technical Security (2), IT or logical security (3), Common Affairs Security (4), Human Resources Security (5), and Legal Security (6). The presented specific areas were grouped according to the conducted risk assessment process and GAP analysis. This architecture model proposed here and in our previous paper (Hajdarevic et al, 2012) is used for ISMS managing purposes. We proposed the central point of data collection from five presented areas responsible for information security support.

3. Proposed infrastructure model

Our infrastructure proposal is based on the usage of already available data stored in database (Microsoft SQL database) from the incident management system used for reporting information security incidents and problems.

Relevant data stored in information security incident management system are related to information security assets mentioned above: people, services, hardware, software, intangibles, and utilities or, more precisely, physical security incidents, incidents related to hardware and software information assets such as virus outbreaks as a side effect of inappropriate usage of information assets such as removable media, visiting Internet sites, etc. Other security incidents not mentioned above are reported on the incident management system distinguishing them by using already available set of definitions which explain and classify incidents.

Figure 2: Infrastructure for data collection and KPI visualisation (Hajdarevic et al, 2012)



Our information security incident management system database contains tables with data which describe the type of incidents, incident locations, incident time occurrences, incident resolution time, person responsible for incident resolution, source of infection for virus outbreak, if applicable, and other data which might be used to help in incident management. Test software was used as a tool for visualisation results of monitoring and improving the system ARIS MashZone (2012). It was necessary to choose the right processes, activities, metrics to measure, and for that purpose relevant data to feed the ARIS Mash zone. By doing this, the goal of successful and constant improvement of the PDCA information security of an organization or a company is much easier to meet.

4. Standard control data determination for measurement process

Information security management involves constant upgrades in terms of ways how metrics has to be established and what measurement processes should take place (Payne & Shirley, 2006). Information security improvement process must be started with the base measurement. While information security is very practical and connected to real world academic researchers also proposing research directions in security metrics (Jasnen, 2009). Standards which belong to ISO 27000 set of standard are ISO 27004:2009 (2009), which can be used to establish a measurement processes within an organisation and ISMS, and NIST guide (Chew et al, 2008) which can be used for specifying meaningful KPI.

ISO 27004:2009 (2009) provides the basic guidance for choosing relevant data and producing relevant results of measurements. This standard (appendix thereto) proposes examples how to create metrics for specific implementation of controls (from ISO 27001:2005 (2005) or other) and how to acquire measured results of implemented controls which need is recognised in risk assessment. There are different sources which can be used as a help to create relevant metrics and measure performance and quality.

Details about how to measure security control effectiveness of general or specific applications in use, implementations for managing application design, process of application implementation and application maintenance can be found in sources such as (Vasudaven et al, 2008).

As explained data used for measurement can be obtained and collected from different organisational units, processes, different levels, or systems of specific organisation. All collected data can be used separately or jointly (aggregately), and by doing that there is great chance to create new knowledge which can then be used at higher levels of the organisation to create appropriate reports and decisions.

An example of choosing specific and relevant data for metrics could be the percentage of critical applications that have separate test environments for the ISO 27001:2005 (2005) control 10.1.4 with the title *"Separation of development, test and operational facilities"*. Because in every business environment critical application where test environment is not used for testing new added features, those new features could create a risk in production system what can create unpredictable production system behaviour.

Using this simple yet effective metrics, it is possible to objectively assess the current risk that critical applications do not have environment for testing purposes.

5. Automated data collection process

After determining which data have to be collected, the best way to collect relevant data is to automatically collect them from specific systems and databases or to automate this process at the highest possible level, if possible. Relevant data have to be presented as metric results of formulas or metric ratios, where metric has to be presented as a number or percentage with appropriate trend indicators (Vasudaven et al, 2008).

6. Model for data calculation

Architecture and infrastructure model for data collection, data mining and presentation of KPI we already presented in (Hajdarevic et al, 2012). Measurement results are intuitive and easy to follow. In this paper, together with presented architecture and infrastructure for data collection, process of data mining, and presenting KPI, additional mechanism for informing about specific thresholds are also presented.

As an example of how architecture and infrastructure could be used, two controls from standard ISO 27001:2005 were chosen to show how data can be used to present the relevant metrics. These controls are: 7.1.3 *Acceptable usage of assets* (MA713) and 10.4.1 *Protection against malicious code*.

As model for KPI creation are used ISO 27001:2005 (2005), 27004:2009 (2009), (Vasudaven et al., 2008) together with 27008:2008 for risks assessment. Metric KPI for the control 7.1.3 *Acceptable usage of assets* is taken number of security malware incidents (MIN) outbreaks as a side effect of unacceptable usage of assets by plugging infected removable media (MIRM) with malware into organisation computer or by accessing infected Internet sites (MIS). By the current results of risk management process below are acceptable values of incidents:

MIN= MIRM+MIS
MA713 = MIN <10 acceptable; MIN <10 not acceptable (Hajdarevic et al, 2012)

For the 10.4.1 *Protection against malicious code* (MA1041) control taken ratio of recognised malware incidents (MIN) by internal anti-virus software, and malwares stopped (MS) at the system gate by using formula, and acceptable limits:

MA1041 = (MIN/MS)*100
MA1041 ≤ 0,1 acceptable; MA1041> 0,1 not acceptable (Hajdarevic et al, 2012)

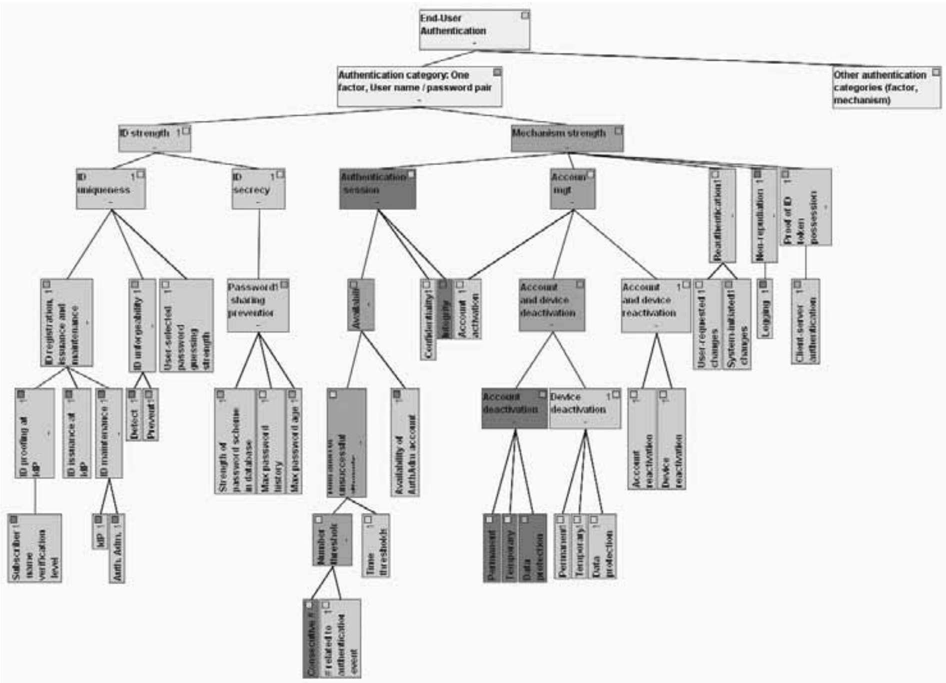
For any other control from standard, data collection and calculation can be used in similar way by choosing what is specific goal of each control. It is important that data are stored in databases or tables so that they can be used for creating relevant metrics.

7. Data mashing using feeds and standard calculations

Real data presentation from production system can be very hard especially to find and present relevant data in bunch of different system which collect that data. One example which shows that data presentation is challenging process because human information security manager is usually overwhelmed with level of information that system create as one which is shown in Figure 2 (Savola & Heinonen, 2011).

By presenting large amount of information to the top management (Security Forum) could result in missing the focus on real issues. Because it can prolong time for making right decisions or to prolong funding new resources needed to support implementation of new systems for controls, which are recognised in preventive or corrective measures as a result of monitoring KPIs. We are proposing approach with two levels of reporting, instead of using more levels of reporting (Savola & Heinonen, 2011) as other system do shown in Figure 2.

Figure 3: Visualisation Tool (Savola & Heinonen , 2011)



High level of reporting is to inform Security Forum if control satisfies desired goals or not.

Low level of reporting informs about details such as details of specific incident, such as incident sources, and is appropriate for IMS. Low level reporting information are used to create proposals for corrective and preventive actions. These actions are later presented to Security Forum for approval.

For the exact implementation for the visualisation and data combination and calculation is used ARIS MashZone (2012) which is commercial software able to search through databases and documents such as Microsoft, Oracle, databases and Excel, CSV, or XML files, HTML web sites, and interpret KPIs. This software can be used manual data feeds.

Aris MashZone use term meshing data (meshing here means: using data from different sources which could ne databases, files, web sites or manual entries and using process of combing, converting, and to execute other operations to present useful data or KPIs). Using different sources (databases, files and manual entries) and combining them together it is possible to discovery new knowledge.

Aris MashZone offer different operations which can be used for data manipulation in database columns or files such as calculation (aggregation, arithmetic, average, round, etc.), change data type, insert, duplicate, delete, rename, change date and time formats and other possibilities too.

As previously presented in section 6. for the control 7.1.3 *Acceptable usage of assets* (MA713) are taken data from columns which contains details: occurrence of the event, type of event (MIRM and MIS), time of start / finish report for each event, open / closed status for each report of event which is monitored dynamically through the time by calculating:

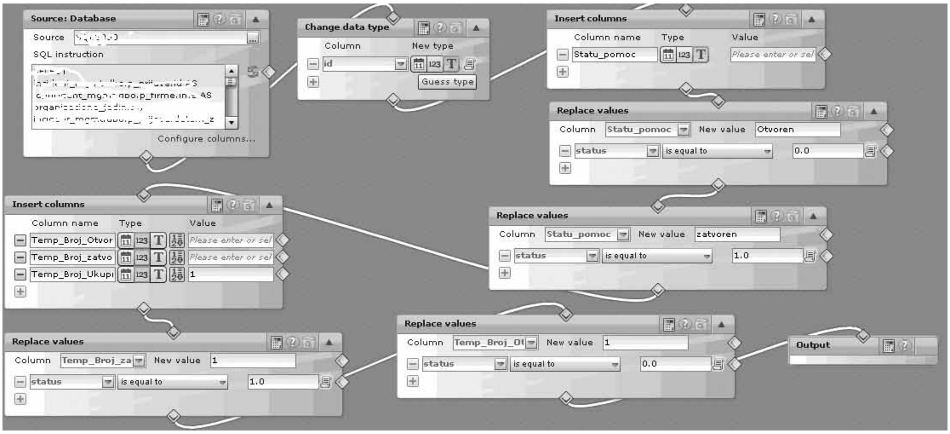
MIN= MIRM+MIS (Hajdarevic et al, 2012)

Similar for the presented in section 6, control 10.4.1 *Protection against malicious code* (MA1041), are taken data from columns in tables and from different Excel files. These sources 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) and that data rae used for this calculations:

MA1041 = (MIN/MS)*100 (Hajdarevic et al, 2012)

ARIS MeshZone (2012) use mechanism called mashup (here mashup means representation of relations and operation on data taken from different data sources) One Mashap for exact data calculation, aggregation is shown in Figure 4. In this mashup are used above presented formulas with a goal to create results in two-dimensional table.

Figure 4: Mashup data feeds (Hajdarevic et al, 2012)



Source: Database

Source [redacted]

SQL instruction

[redacted]

Configure columns...

Change data type

Column	New type
id	

Guess type

Insert columns

Column name	Type	Value
Statu_pomoc		Please enter or sel

Replace values

Column Statu_pomoc New value Otvoren

status is equal to 0.0

Replace values

Column Statu_pomoc New value zatvoren

status is equal to 1.0

Insert columns

Column name	Type	Value
Temp_Broj_Otvor		Please enter or sel
Temp_Broj_zatvo		Please enter or sel
Temp_Broj_Ukupı		1

Replace values

Column Temp_Broj_za New value 1

status is equal to 1.0

Replace values

Column Temp_Broj_Ot New value 1

status is equal to 0.0

Output

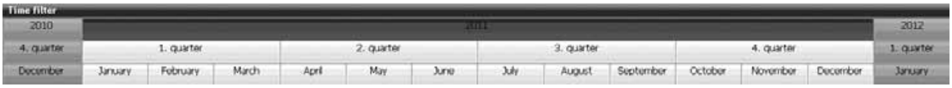
Presentation and visualisation results can be done by using this resulting two-dimensional table by filtering, combining, aggregating data from different sources and different units and levels of organisation.

8. KPI visualisation

Here the purpose of data collection is visualize KPI results in specific time window creating specific trends.

Specific time window can be set up to monitor specific trends such as yearly, quarterly, monthly, weekly, daily, or other KPI result representation for all or specific categories as it is shown in Figure 5.

Figure 5: Yearly, Quarterly, monthly data (Hajdarevic et al, 2012)



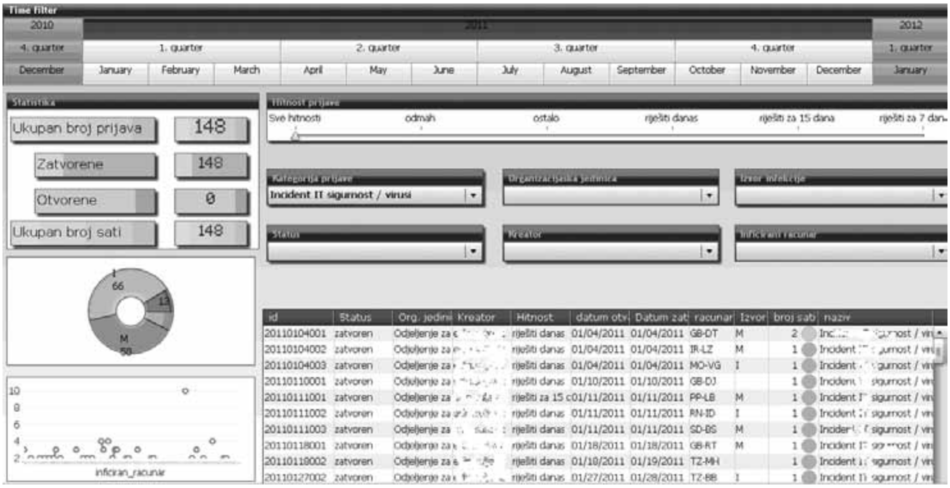
Time filter

2010	2011												2012
4. quarter	1. quarter			2. quarter			3. quarter			4. quarter			1. quarter
December	January	February	March	April	May	June	July	August	September	October	November	December	January

Information which can be presented might be: top infected units, names of responsible employees, physical locations affected computer equipment, and other information assets.

Monitoring trends of KPIs through the time offers advantage of adjusting metric settings for detecting specific problems and resolving them proactively avoiding future occurrences.

Figure 6: KPI visualisation window (Hajdarevic et al, 2012)



Ukupan broj prijava 148

Zatvorene 148

Otvorene 0

Ukupan broj sati 148

Kategorija prijave: Incident IT sigurnost / virusi

Organizacijska jedinica:

Izvor infekcije:

Status:

Kreator:

Inficirani racunar:

id	Status	Org. jedini	Kreator	Hitnost	datum otv	Datum zat	racunar	Izvor	broj sat	naziv
20110104001	zatvoren	Odjeljenje za	[redacted]	riješiti danas	01/04/2011	01/04/2011	GB-DT	M	2	Inc[redacted]gurnost / vir
20110104002	zatvoren	Odjeljenje za	[redacted]	riješiti danas	01/04/2011	01/04/2011	IR-LZ	M	1	Incident [redacted]gurnost / vir
20110104003	zatvoren	Odjeljenje za	[redacted]	riješiti danas	01/04/2011	01/04/2011	MO-VG	I	1	Incident [redacted]gurnost / vir
20110110001	zatvoren	Odjeljenje za	[redacted]	riješiti danas	01/10/2011	01/10/2011	GB-DJ		1	Incident [redacted] sigurnost / vir
20110111001	zatvoren	Odjeljenje za	[redacted]	riješiti za 15 c	01/11/2011	01/11/2011	PP-LB	M	1	Incident [redacted] sigurnost / vir
20110111002	zatvoren	Odjeljenje za	[redacted]	riješiti danas	01/11/2011	01/11/2011	RN-ID	I	1	Incident [redacted] sigurnost / vir
20110111003	zatvoren	Odjeljenje za	[redacted]	riješiti danas	01/11/2011	01/11/2011	SD-BS	M	1	Incident [redacted] sigurnost / vir
20110118001	zatvoren	Odjeljenje za	[redacted]	riješiti danas	01/18/2011	01/18/2011	GB-RT	M	1	Incident [redacted] sigurnost / vir
20110118002	zatvoren	Odjeljenje za	[redacted]	riješiti danas	01/18/2011	01/19/2011	TZ-MH		1	Incident [redacted] sigurnost / vir
20110127002	zatvoren	Odjeljenje za	[redacted]	riješiti danas	01/27/2011	01/28/2011	TZ-BB	I	1	Incident [redacted] sigurnost / vir

New feature of the reporting approach presented her might be notifying about thresholds reached defined in acceptable levels for specific KPI presented in section 6.

9. Conclusions

In the papers (Vasudaven et al., 2008), (Leszczyna et al., 2011), (Savola & Heinonen, 2011) are presented partial solutions to crate and monitor overall information security KPIs, here is presented holistic approach including architecture and infrastructure for data collection, mining and KPI visualisation. For relevant KPI visualisation relevant data sources are needed such as databases which belongs to systems which collects data relevant for five areas which could be find in many Central Banks

Similar reports could be created with open source solutions such as not only Report for this paper are created by commercial software like MashZone (2012) used here only for test purposes, but other commercial solutions could be used such as HP Executive scorecard (2012) or with very limited possibilities ReportManager (2012) compared to other two surroundings mentioned above.

References

1. 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.
2. Chew E., Swanson M., Stine K., Bartol N., Brown A., and Robinson W., (2008) Performance Measurement Guide for Information Security. NIST, July 2008, Available at: http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf, [Accessed on: 25.1.2012]
3. Duremeyer Karin, (2004) 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,%20 Lutz.ppt [Accessed on: 10.1.2012]
4. Hajdarevic K., Pattinson C., Kozaric K., Hadzic A., Information Security Measurement Infrastructure for KPI Visualization, pp MIPRO 2012/ISS, pp 1877 – 1882
5. HP Executive Scorecard, (2012) 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]
6. ISO 27001:2005, (2005) Information Technology – Security techniques – Information security management – Requirements, ISO / IEC 27001:2005, 31.6.2004 First edition.
7. ISO / IEC 27004:2009, (2009) Information Technology – Security techniques – Information security management – Measurement, ISO / IEC 27004:2009, 15.12.2009 First edition.
8. Jansen W., (2009) Directions in Security Metrics Research, National Institute of Standards and Technology, US Department of Commerce. NISTR 7564. April 2009.
9. Leszczyna R.I.N., Fovino M., Masera, (2011) 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.
10. MashZone 2012, Available at: www.mashzone.com [Accessed on: 10.1.2012]
11. Moen R. and Norman C, (2009)Evolution of the PDCA Cycle, Available at: http://pkpinc.com/files/NA01MoenNormanFullpaper.pdf [Accessed on: 13.7.2012]
12. Payne C. Shirley, (2006) 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]

13. Report Manager, (2012) Available at: http://reportman.sourceforge.net [Accessed on: 10.1.2012]
14. Savola R. M. Heinonen P.A, (2011) Visualisation and Modeling Tool for Security Metrics and Measurements Management. Information Security South Africa (ISSA) 2011 IEEE, ISBN 978-1-4577-1481-8.
15. Vasudaven V, Mangla A, Ummer F. Shetty S. Pakala S. Anbalahan S., (2008), Aplication Security in the ISO27001 Environment, 2008. Governance Publishing. ISBN 978-1-905356-35-5.
16. Watkins S., (2012) UK crash 'worsened by Libor misquotes' - Barclays boss's shock email to Mail on Sunday, Available at: http://www.dailymail.co.uk/news/article-2167091/UK-crash-worsened-Libor-misquotes--Barclays-bosss-shock-email-Mail-Sunday.html [Accessed on: 13.7.2012]