GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Measuring effectiveness in Information Security Controls

GIAC (GSEC) Gold Certification

Author: Manuel Humberto Santander Peláez, manuel@santander.name
Advisor: Rick Wanner

Accepted: April 5th 2010

Abstract

The main purpose of the Information Security Analyst is to control the exposure to information security risks. However, the information security budget is not unlimited and there is increasingly a need to justify the return on investment for the controls implemented in our companies. How can we show the effectiveness of those controls? One way is to perform a risk analysis process to determine the controls to be implemented. The risk analysis process defines the critical variables that, when monitored, shows the risk exposure level and then determine the metrics that will measure the effectiveness of the controls. This paper shows a proposal on how to measure the effectiveness of implanted information security controls as part of the corporate Information Security process.

© 2010 SANS Institute, Author retains full rights.

© 2010 The SANS Institute Author retains full rights.

1. Introduction

The risks in the business environment of companies and international regulations have made companies incorporate as business process the aspect of information security.

Like all processes, it needs to get assigned resources and budget to ensure proper implementation. Because the objective of the security process is to minimize exposure to risk it is important to determine the effectiveness of the implemented controls.

How do you measure if the security controls in place are effective? How do you justify the budget to augment or improve existing controls? It is important to show the organization that the requested funds will be invested in preventing the issues that can materialize an information risk against any of the core business processes.

This paper illustrates how to define indicators to measure the exposure to information risks in the company processes.

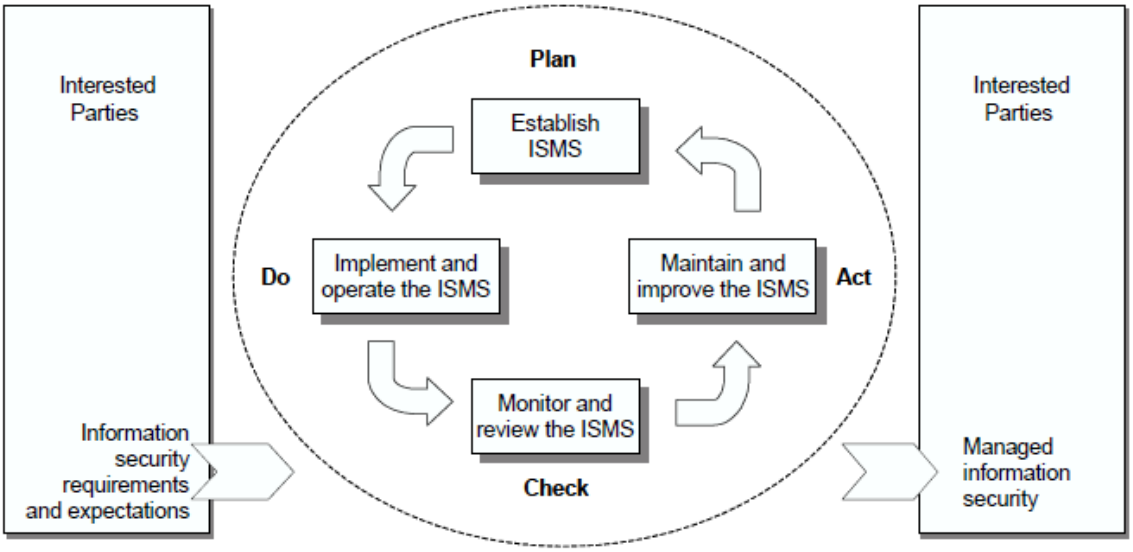
2. Information Security Management System (ISMS)

The Information Security Management System (ISMS) standard provides a framework for information security risk management within organizations. The purpose of this system is to identify and minimize risks when handling information within the company's processes, so the confidentiality, integrity and availability of the information are preserved, maximizing its value as input to the value chain processes within the corporation.

The ISMS suggests a Plan, Do, Check, Act (PDCA) (ISO, 2005) cycle within the organization based on the following scheme:

© 2010 SANS Institute, Author retains full rights.

© 2010 The SANS Institute Author retains full rights.



Source: ISO/IEC FDIS 27001(ISO, 2005)

The objectives for each step of the cycle (ISO, 2005) are:

- Plan: To establish information security policy and objectives to manage risk and improve the level of risk exposure.
- Do: Implement the security controls planned for the ISMS in accordance with established information policy and security objectives.
- Check: To evaluate and measure process performance and controls against established guidelines.
- Act: Take corrective and preventive actions based on the results of verification in order to implement a continuous improvement to the ISMS.

As part of this process, the company must implement the necessary security controls and the required measurement to lower the risk exposure of the organization to an acceptable level. Because many company executives do not understand the need of measure for security control performance, attaining resources can often be a difficult task requiring a significant number of justifications just to determine if information security controls are necessary and good for business.

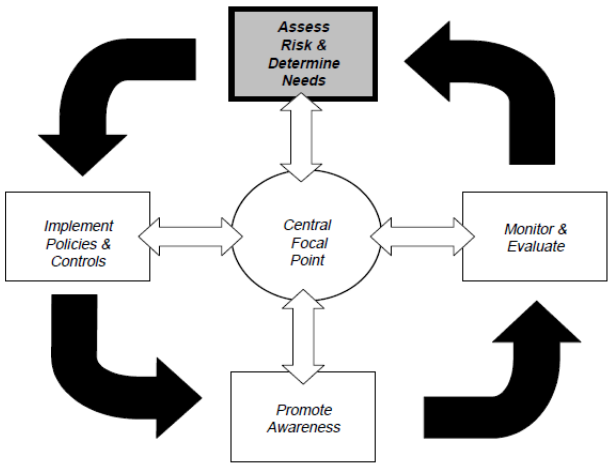
In order to provide convincing arguments to management to initiate an information security program, Information Security Officers must identify risks to organizational processes and develop a measurement system capable of determining the

© 2010 The SANS Institute Author retains full rights.

effectiveness of controls introduced in accordance with Annex A of the ISO 27001 standard or other relevant standard.

3. Assessing Information Security Risks

The information security risk assessment is a subset of the integrated risk management system (U.S. Government Accountability Office, 1999). This system provides a risk management cycle with the following items:



Source: Information Security Risk Asessment – United States General Accounting Office

http://www.gao.gov/special.pubs/ai00033.pdf (U.S. Government Accountability Office, 1999)

- Risk assessment: The mechanism that provides decision makers the information they need to understand the risk factors that may adversely affect the operations and affect the outputs of the company's processes. This includes identification of threats, estimating the probability of occurrence of the threats based on historical data, identification and cataloging of the value, criticality and sensitivity of the assets that may become affected, an estimate of potential losses, identification of cost-effective actions to mitigate the risks and document the results and implementation plan for the resulting controls (U.S. Government Accountability Office, 1999).

© 2010 The SANS Institute Author retains full rights.

- Implementations of policies and controls: For each identified risk that is classified as a high impact on organizational processes, the company must implement policies and controls that will diminish the risk to an acceptable level (U.S. Government Accountability Office, 1999)
- Promote awareness: The risks are less likely to occur if users are aware of how they can occur. Regular training is needed to maintain current awareness of risk management policies in the organization (U.S. Government Accountability Office, 1999).
- Monitor and evaluate: The organization shall specify the critical risk factors and indicate the potential level of exposure. These factors are what determine the implementation of controls and, therefore, must determine its behavior over time to determine whether the level of risk exposure has increased or decreased (U.S. Government Accountability Office, 1999).

However, assessing the risk exposure can be difficult, since the data necessary for assessing the likelihood and impact of each risk are limited because the root causes are constantly changing. For example, how easy can the company determine the cost associated with the loss of customer confidence? If there is a leak of company information, how easy can the company quantify the impacts on business processes? How easy is estimating the likelihood of an attack and the cost of damage, loss or interruption of service caused by events that exploit existing security vulnerabilities? (U.S. Government Accountability Office, 1999)

As explained above, the budget is an important constraint when devising controls for information security. For the sake of using it properly and to add value to the organization, you must define and measure to establish the effectiveness of security controls in the required risk reduction.

Determining the effectiveness of controls is a fundamental exercise used to assess risk, but we must also take into account that the measurement of efficiency has a number of costs involved, in the end increasing the total cost of ownership of infrastructure and therefore affects the cost of goods and services originating in the organization. The

© 2010 The SANS Institute Author retains full rights.

measurement scheme chosen should be effective and efficient enough to not blur the use of resources.

The resulting controls can be too much and we risk not focusing on the critical business processes. To avoid losing the focus should prioritize the analysis of Key Performance Indicators, which are a quantifiable measurement that can be used to track the progress in achieving important goals within a company. (DSM, 2009).

Information Security teams need to gather the key risk indicators, to measure how risky are activities done in the organization (QFinance, 2010). When they have available both inputs, they must make a map that show how the KRI can affect KPI and what impacts can cause to processes in the organization (Tucci, 2009). Following tasks can help also:

- Formalize a risk and security program.
- Don't use operational metrics in executive communications.
- Link risk management initiatives to corporate goals.
- Communicate to executives what works and doesn't work.

4. Associated measurement control costs

Implementing metrics involves a series of costs, which require an investment in technology, people and processes as well:

- Investment in technology: To minimize risks, the technology component is essential because the devices deployed in the infrastructure, such as firewalls, intrusion detection systems, intrusion prevention systems and anti-malware systems, all generate a large amount of data, which need to be processed by log correlation devices, generating valuable information on the successful or unsuccessful attempts of violation of a specific control set.
- Investing in people: The way people work changes when the ISMS is implemented. People must be aware of their role in the management of

© 2010 The SANS Institute Author retains full rights.

© 2010 SANS Institute, Author retains full rights.

information security, can use the deployed technologies properly and minimize the time of the execution of processes, in both cases to minimize the likelihood of threat realization. This involves conducting workshops and training courses to further measure the weight of people in the security control performance inside the organization.

- Processes: Given that the information security definitions require changes to the way people work, to implement a control it must be clearly defined what must be protected, and to what extent, in order to generate information on their performance. Based on the information security policies, the ultimate goal is to define the process so that it is possible to quantify the effectiveness of the policies in terms of protection of information security.

5. Measuring Controls

To measure the controls we need to develop good quality metrics for each one of them. Those good quality metrics need to have the following characteristics:

- It must be universal, which means that can be applied regardless of the architecture, code, interface or system conditions. A metric is universal if it is composed of a clearly defined set of variables that can be used in any type of ISMS to which you want to apply the measurement. (International Function Point Users Group, 2002)
- It must yield significant results with respect to the issue it seeks to measure. Hence the importance of defining a set of metrics that are useful to the assessment group to get what you really want to know, without elaboration and without the need for further information. (International Function Point Users Group, 2002)
- It must be accurate and represent what information security officers really want and need to know. A metric should not divert attention to another aspect other than the purpose for which it was intended. Moreover, it should accurately portray the results, avoiding bias, both by the group

© 2010 The SANS Institute Author retains full rights.

responsible for the measurement and the decision makers. Obtaining results should be feasible, i.e., it should be possible to obtain the data and variables involved in the measurement, so as to optimize resources and avoid waste of effort, time and money on measurements impossible perform. (International Function Point Users Group, 2002)

- Must be reproducible, so that different people at different times can make the same measurement. It is vital the metric be consistently repeatable, regardless of who made the measurement or the moment in time that the measurement takes place, provided that the conditions for measurement are preserved. (International Function Point Users Group, 2002)
- It must be objective, i.e. must not be tied to variable factors such as the knowledge of people, the ability to memorize, product perception, among others, avoiding subjective factors that could skew or corrupt the results. (International Function Point Users Group, 2002)
- It must be impartial. A metric must be fair and equitable, must have a clearly defined set of values with which one can determine if the result is acceptable or not, and to know the level and/or the trending of attributes of the system. (International Function Point Users Group, 2002)

ISO27004 defines a measurement method with the following steps (ISO, 2009):

- Complete list of the controls implemented in accordance with Annex A of ISO27001 standard
- Method for measurement of attributes associated with controls
- Base measure for the control attributes
- Generation of the indicator

According to the result of the risk matrix, you must select those controls that have the greatest ability to decrease the risk of exposure to the process information. The controls consist of variables, which determine its level of functioning. Those variables are called attributes.

© 2010 The SANS Institute Author retains full rights.

The attributes are proxies for control in risk exposure. The state of the attributes of control implies a specific level of risk, which is measured through a specific mechanism. Some of those mechanisms are (ISO, 2009):

- Questionnaires and personal interviews
- Audit reports
- Records of events

The result of the implementation of the measuring mechanism is to control the attributes of the call based measures. These measures when applied to the basic attributes of the same risk can be combined using techniques of weighted average, simple average, percentages, among others. These combined measures are called derived measures and are the main input for the creation of indicators (ISO, 2009).

The indicators must express the current level of security compared to the desired security level, based on the level of residual risk accepted by the organizational processes. The goal of the indicator is to reflect the level of risk exposure by the current implementation status of a control (ISO, 2009).

6. Case Study

We will translate all these concepts into a practical example. For a utility company, the core of their business is uninterrupted delivery of utility services (electricity, water supply, telecommunications, gas, etc.) and the threats to control are those that put at risk the delivery of these services.

Consider the case of the processes required to operate an electric power transmission system. Some of the Key Performance Indicators associated to the process are:

- Members of the public injured as a direct result of our operations (number of fatalities) (National Grid, 2008)
- Employee lost time injury frequency rate (National Grid, 2008)

© 2010 The SANS Institute Author retains full rights.

- Electricity delivered by the electricity transmission system as a proportion of electricity demanded (National Grid, 2008)
- MWh lost on our electricity transmission system (National Grid, 2008)
- Average time the average customer is without power over the year from our electricity distribution network (National Grid, 2008)

Some of the information security risks (KRI) to this process are:

- Interruption of electrical service, by opening a line or transformer critical to the transmission system: This risk may materialize at some type of intrusion to the IT components of the Supervisory Control and Data Acquisition (SCADA) system or other equipment that manages the electrical system components.
- Injury or death to employees and contractors by exposure to energized equipment while operating the substation or in the SCADA system: This risk may materialize by manipulating the SCADA system or the control equipment that manages the electrical system.
- Increased expense due to equipment damage while in operation or standby: The investments made to operate an electrical system are enormous, as the cost of acquisition, installation and commissioning of equipment is high because of their degree of specialization. Because control devices are very sensitive and easily damaged by any uncontrolled excess voltage, which can be controlled from the SCADA system, what would happen if the control equipment used for transmission is damaged due to an order sent from a compromised SCADA system? The insurance deductible would be high and the financial position of the company could be seriously affected.

These risks may materialize for causes that affect the SCADA system or the electrical control system. In this case, the causes are:

- Lack of security patches: If proper patch management procedures are not in place there may be vulnerabilities that attackers can exploit.

© 2010 The SANS Institute Author retains full rights.

- Unlimited Access: The SCADA system and the electrical system control components are delicate and are prone to stop functioning at the slightest disturbance. If an element of the SCADA system or control equipment is affected by a denial of service attack this can mean the interruption of electrical service for an entire country.
- Access control weaknesses: The SCADA system and control equipment were designed to operate with high performance, because of this the deployed security controls are minimized. Many of the devices do not even have account management capabilities, potentially leaving the power transmission system in a vulnerable state. It is important to note that in this type of system operational efficiency is vital, and if a control that can be established by setting a device is detrimental to the efficiency of the device's operation, it cannot be implemented and the cause must be minimized by other controls.
- Attacks from malicious software: viruses, Trojans, spyware and other malicious software can cause service disruptions and even the entire system can be enabled for remote management.

As seen previously, KRI and KPI match. According to the defined risk management cycle, we must now define the specific controls to mitigate the limitations that may lead to the materialization of risks. In this case, the recommended controls are:

- A perimeter security system consisting of firewalls and IPS, where only necessary access is granted to minimize the impact on the communication between the management components and the operation of the electrical system, the logging of access, authorized and unauthorized, to the SCADA system and control equipment and protect all devices from application-level attacks.
- An anti-malware solution which minimizes the chance of infection and intrusion into the SCADA system and control equipment.

© 2010 The SANS Institute Author retains full rights.

A patch management process to ensure all available patches are tested and deployed in a timely manner and do not affect the equipment operation.

To avoid an excessive increase in costs associated with measuring the performance of the controls, we must define what level of risk that the process can tolerate and from this input define a measurement scheme to perform control measurement.

The scale proposed for the analysis is as follows:

Consequence	Value	Criteria
Catastrophic	**5**	**a)** Generates loss of confidentiality of information that can be useful for individuals, competitors or other internal or external parties, with non-recoverable effect for the Company. **b)** Generates loss of integrity of information internally or externally with non-recoverable effect for the Company. **c)** Generates loss of availability of information with non-recoverable effect for the Company.
Higher	**4**	**a)** Generates loss of confidentiality of information that can be useful for individuals, competitors or other internal or external parties, with mitigated or recoverable effects in the long term. **b)** Generates loss of integrity of information internally or externally with mitigated or recoverable effects in the long term. **c)** Generates loss of availability of information with mitigated or recoverable effects in the long term.
Moderate	**3**	**a)** Generates loss of confidentiality of information that can be useful for individuals, competitors, or other internal or external parties, with mitigated or recoverable effects in the medium term. **b)** Generates loss of integrity of information internally or externally with mitigated or recoverable effects in the medium term. **c)** Generates loss of availability of information with mitigated or recoverable effects in the medium term.

© 2010 The SANS Institute Author retains full rights.

Consequence	Value	Criteria
Minor	**2**	**a)** Generates loss of confidentiality of information that can be useful for individuals, competitors, or other internal or external parties, with mitigated or recoverable effects in the short term. **b)** Generates loss of integrity of information internally or externally with mitigated or recoverable effects in the short term. **c)** Generates loss of availability of information with mitigated or recoverable effects in the short term.
Insignificant	1	**a)** Generates loss of confidentiality of information that is not useful for individuals, competitors or other internal or external parties. **b)** Generates loss of integrity of information internally or externally with no effects for the company **c)** Generates loss of availability of information with no effects for the company.

According to the proposed scale, the risks presented for the power transmission network example measure as high. Hence, we implement an event correlation system that enables us to proactively detect security intrusions and, in the worst case, that permits compilation of evidence for investigative purposes or to build a computer forensics case to determine what happened to prevent it from recurring and to potentially undertake legal action if required.

To verify the effectiveness of controls, we measure how much the control decreases the probability of realization of the described risks. According to the methodology described, we must determine what attributes belong to the implemented controls which are relevant to measure. The attributes must be significant in determining the increase or decrease of risk. The following is the array of causes, controls implemented and measurement attributes:

Risk cause	Control	Attribute
Lack of Security Patches	Patch management process	List of missing security patches that does not affect the performance on SCADA and control equipment
		Log of successfully installed security patches on SCADA and control equipment

© 2010 The SANS Institute Author retains full rights.

Risk cause	Control	Attribute
Unlimited access	Perimeter security system	Logs of authorized and unauthorized connections
Access Control Weakness, Unpatched systems because of performance issues		Logs of application-level attacks
Attacks from malicious software	Antimalware solutions	Log of actions taken by anti-malware software regarding malicious software attacks

Given that the impact on the risk was described as catastrophic, the risk likelihood should be mitigated using all reasonable controls, we need the information security control performance to be excellent. Therefore, we design the base measure from the control attributes. The obtained results must show the control performance. The proposal is:

Attribute	Base Measure	Measure Scale
List of missing security patches that does not affect the performance on SCADA and control equipment	Number of patches successfully installed on SCADA and control systems	0
Log of successfully installed security patches on SCADA and control equipment		
Logs of authorized and unauthorized connections	Number of security incidents caused by attacks from the network	All occurred
Logs of application-level attacks	Number of security incidents caused by application-level attacks	All occurred
Log of actions taken by anti-malware software regarding malicious software attacks	Number of security incidents caused by malicious software	All occurred

© 2010 The SANS Institute Author retains full rights.

These measures should be expressed numerically, since such criteria as "all occurred" lends itself to subjective interpretation of control performance. Given that the amounts presented are variables, the percentage is an illustrative measure of performance for controls. What follows are derived measures as percentages from the base measures and the proposed measurement scale:

Base Measure	Derived measure	Expected measure
Number of patches successfully installed on SCADA and control systems	Number of patches successfully installed on SCADA and control systems / Number of issued security patches for SCADA and control equipment	> 95%
Number of security incidents caused by attacks from the network	Number of security incidents caused by attacks from the network / Number of effectively detected attacks from the network	0%
Number of security incidents caused by application-level attacks	Number of security incidents caused by application-level attacks / Number of effectively detected application-level attacks	0%
Number of Security incidents caused by malicious software	Number of Security incidents caused by malicious software / Number of effectively detected attacks caused by malicious software	< 3%

If the measure is equal to or below the recommendation, we can say that the risk is adequately controlled, according to the classification established at the start. The proposed indicators are the trends of the derived measures and they must be within the same measurement scale in order to establish that the risk is adequately controlled. The following are proposed:

Derived measure	Indicator
Number of patches successfully installed on SCADA and control systems / Number of issued security patches for SCADA and control equipment	Trend in security patches installation

Manuel Humberto Santander Peláez, manuel@santander.name

© 2010 The SANS Institute Author retains full rights.

Number of security incidents caused by attacks from the network / Number of effectively detected attacks from the network	Trend in detection of network attacks
Derived measure	**Indicator**
Number of security incidents caused by application-level attacks / Number of effectively detected application-level attacks	Trend in detection of application attacks
Number of Security incidents caused by malicious software / Number of effectively detected attacks caused by malicious software	Trend in detection of malicious software attacks

7. Conclusion

The ISO27001 standard was adopted to assist organizations in reducing security risks that may affect information assets. Given existing internal constraints such as budget and operational procedures, it is necessary to seek to implement security controls that allow diminishing the risks but there is also a cost effective way that will not undermine the financial solvency of the business.

The result obtained by the risk analysis identifies the controls to be implemented. The risk classification obtained by the analysis, will define the nature of the measurement mechanisms employed to attempt to measure the effectiveness of controls.

The key to the metrics definition is the correct definition of the critical attributes of the control to measure the risk exposure of the company. The metrics must be accompanied by a measurement scale that permits the identification of the current state of the risk level of the company. To avoid subjective measures, they should be expressed as percentages where the control variable should be to avoid risk exposure.

To determine trends, it is essential to make measurements at consistent time intervals and record the results. These graphs allow to quickly determining breakpoints in risk exposure to make the necessary corrections quickly.

© 2010 The SANS Institute Author retains full rights.

The process of measuring the performance of controls is not the same for all companies or the same for the processes within the organization. Each case must determine indicators to establish the efficiency of the security process in reducing the risks.

8. References

ISO. (2009). *ISO/IEC 27004:2009*. Geneva, Switzerland: International Standard Organization.

ISO. (2005). *ISO/IEC 2700:2005*. Geneva, Switzerland: International Standard Organization.

U.S. Government Accountability Office. (1999). *Information Security Risk Assessment*. Retrieved Abril 27, 2010, from GAO Website: http://www.gao.gov/special.pubs/ai00033.pdf

International Function Point Users Group. (2002). *IT Measurement practical advice from the experts*. Boston, MA: Addison-Wesley.

Tucci, Linda. (2009, July 1). *Using Key risk indicators to sell your information security program*. Retrieved from http://searchcio-midmarket.techtarget.com/news/article/0,289142,sid183_gci1360671_mem1,00.html?ShortReg=1&mboxConv=searchCIO-Midmarket_RegActivate_Submit&

DSM. (2009, September 1). *Glossary*. Retrieved from http://www.dsm.com/en_US/html/sustainability/glossary.htm

QFinance. (2010, June 22). *Setting Up a Key Risk Indicator System*. Retrieved from http://www.qfinance.com/operations-management-checklists/setting-up-a-key-risk-indicator-system

National Grid. (2008). *Key performance indicators*. Retrieved from http://www.nationalgrid.com/corporate/Our+Responsibility/Reporting+our+Performance/perfmeas/Key+performance+indicators/

© 2010 The SANS Institute Author retains full rights.