International Journal of Enhanced Research in Management & Computer Applications
ISSN: 2319-7471, Vol. 6 Issue 8, August-2017, Impact Factor: 3.578

Using the BS 7799 to improve Organization Information Security

.

Gaurav Malik

E-Mail: gauravrmalik@gmail.com

ABSTRACT

In this paper i have explained how we can we improve information security process of an organizations by using BS 7799 I have also explained the various sub stages of the ISMS planning phase and compliance of BS 7799-2

Keywords: BS 7799, Security

INTRODUCTION

Towards the BS 7799-2 compliance

The whole process of making organizations more secure in an information security point of view can be divided into four steps that are executed in a cycle. These steps are presented in a Figure 4. In this thesis work, the primary area that will be focused on is the planning phase because the organization that is evaluated according to the BS 7799 is in the first stage of the process. In addition, the actual standards ISO/IEC 17799 and BS 7799-2 only cover these three other stages very briefly. The different sub stages of the planning process are described detailer later in this chapter and after those, there is a brief intro to the other three stages of the ISMS process. [1]

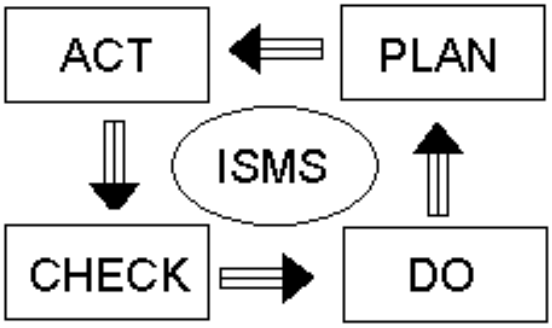

Figure 1: ISMS cycle [5]

Different sub stages of the ISMS planning phase

There are six different steps on ISMS planning phase. These different phases and their sequence can be found from the Figure 2. In the chapter two, there was a short intro to all of these steps and how they are defined in BS 7799-2. In this chapter all of these six chapters are gone throughmore accurately and there the point of view is not only chosen from the standard but from other sources and from the own experiences also. [2]

Define the policy

As written already earlier the information security policy is the main building block of the corporate information security. The most important thing in security policy is that the management of the organization approves it and every employee inside organization is aware of it. The information policy should at least cover these areas. [2]

- A definition what is information security. Information security is usually defined by three words confidentiality, availability and integrity. The meaning of these three words should be clear to everyone after reading the section that defines information security. Access control is the forth member of this group but it usually left away from definition of information security. [2,6]
- A statement of management's intent. This part's purpose is to support the goals and principles of the information security policy. The part needs to offer a clear picture why this document is important and why it should be well understood by every member of the staff. [2,6]
- A brief explanation of the security policy's principles. In this section at least following principles should be described. First is the compliance with legislative and contractual requirements. What are the official rules that need to be followed? The second one is the security education requirements. What are the minimum requirements for the members of the staff? The third one is instructions how viruses and malicious software are prevented from breaching into intranet and how is internal detection of such software done. The forth is ensuring the business continuity. How are key elements of the business process protected? What are the most important processes that need protection? The last but not least important are the rules for the case that there are violations against the rules defined in security policy. What are the actions if somebody deliberately breaks these rules and makes organizations key processes vulnerably? [2,6]
- A definition of the responsibilities in information security. There should be a chapter in security policy that defines who is responsible of the certain areas including the management of the security policy. In the case of incidents, there should be also be defined a person who is responsible of reporting these incidents. [2,6]
- References to the supporting documentation. Information security policy should not be longer than three pages when printed. That is why it cannot hold all the information but just the main features. To make this policy as efficient as possible guidelines and more documentation is usually needed and security policy should have clear instructions where to find these documents. [2,6]

To summarize the qualities that are important to information security policy there could be three rules: keep it simple, keep it short and keep it available. A good example of the security policy can be found from the University of Florida, which security policy that can be read from the address found from reference number 17. [2,6]

Define the scope

The scope of the ISMS defines what is the actual target of the process improving the information security. There has been some discussion that the scope should be defined before defining the policy. By doing this policy could be written more accurately to the specific needs considering the actual part ISMS process is focused on. On the other hand, information security policy should be same for the whole organization. If there would be different policies for each individual department inside the organization the power of information security policy would decrease. [1]

The scope defines what the target of ISMS is. Usually the scope can be defined to be the whole organization, but sometimes it is more beneficiary to focus on some specified area. When the target of ISMS is defined, it is necessary to choose the areas that are focused on. These areas could for example be databases, information, personnel, facilities, applications hardware and software or communications hardware and software. The size of the target is one of the main factors that define how specified data ISMS produces. If the target were, just single service the data is more accurate versus the case the target would be the whole organization. The choices made in this step might have major effect to the results produced in later steps. [1, 2, 3]

Undertake a risk assessment

The function of the risk assessment is to discover all the risks that have a notable effect to the organization. The first step of this process is to find out all the risks that organization faces. The second step is to find out what risks are actual ones. [2, 3]

Risk identification

To find all the risks that the organization faces is a difficult task. To accomplish this task several different solutions are available. One of them is an existing risk list that holds a comprehensive list of threats usual to certain type of industries. The list is analysed with a team that has members from different departments inside the organization and possible risk that could also be real in the organization are chosen. This method has an advantage that it usually goes through all the areas of the business but its disadvantage is that it does not produce risk list that would be very specific to the certain organization. Risk list sometimes also steers the focus only to certain types off risks. An example of this kind of risk list can be found

from Table 1 where the source of the threat is human. This sample list only provides the threats but the actual risks can be derived from them. Usually risk list are a lot detailer but this list shows some example of what could be the possible format of the risk list. [7]

Table 1: Possible human threats [23]

Threat Source	Motivation	Threat Actions
Hacker, cracker	Challenge Ego Rebellion	• Hacking • Social engineering • System intrusion, break ins • Unauthorized system access
Computer criminal	Destruction of information Illegal information disclosure Monetary gain Unauthorized data alteration	• Computer crime (e.g., cyber stalking) • Fraudulent act (e.g., replay, impersonation, interception) • Information bribery • Spoofing • System intrusion
Terrorist	Blackmail Destruction Exploitation Revenge	• Bomb/Terrorism • Information warfare • System attack (e.g., distributed denial of service) • System penetration • System tampering
Industrial espionage (companies, foreign governments, other government interests)	Competitive advantage Economic espionage	• Economic exploitation • Information theft • Intrusion on personal privacy • Social engineering • System penetration • Unauthorized system access (access to classified, proprietary, and/or technology-related information)
Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)	Curiosity Ego Intelligence Monetary gain Revenge Unintentional errors and omissions (e.g., data entry error, programming error)	• Assault on an employee • Blackmail • Browsing of proprietary information • Computer abuse • Fraud and theft • Information bribery • Input of falsified, corrupted data • Interception • Malicious code (e.g., virus, logic bomb, Trojan horse) • Sale of personal information • System bugs • System intrusion • System sabotage • Unauthorized system access

Another solution that can be used in risk identification is JyrkiKontio's "Riskit"-method. In this method, also a group of people from different departments inside the organization is used to evaluate the risks. The first step in this method is brainstorming session where every member of team writes down independent from the other members as many risks as possible. The next step is to collect the risks together. After this, the risks are organized to the groups based on what area they represent. These different areas could be physical, personnel, legislative, etc. This step is called affinity-grouping part. In this phase, the possible doubles are removed and more risks can be written down. This method should produce variety of

risks from different sectors. The downside is that when members of risk management group do not have enough experience there could be some critical threat that is not written down. The method is presented in detail on the publications made by JyrkiKontio that can be found from reference 5. [5]

Both of these two methods introduced have their advantages and disadvantages. "Risk-It"-methods might work better on small projects and the "risk list"-method could be better when the target is larger. One solution could be combining these both. First start with the "Risk-It"-method, then check the results with risk list, and add possible risks that were not founded during the brainstorming and "affinity-grouping" phase. [5, 7]

RISK CLASSIFICATION

There are two possibilities to do this risk classification to the risks that are real and to the ones that need no attention. Every risk has two main properties. The first one is the probability of the risk and the second one is the effect of the risk. According to these two properties, risks can be divided into two categories that are called as the applicable or non-applicable risks. Applicable risks need to be controlled and actions should be made to get these risks under acceptable level that is defined in organizations information security policy. [1, 5]

Gamma Secure Systems Limited [1] has presented a model where risks are categorized with a help of two dimensional graph. An example of this graph can be found from the Figure 5. The main idea is to define a level of possibility and a level of effect that are considered to be two minor to take actions with. If the risk is located under either of these two lines in a graph it is not taken under evaluation in later steps of the ISMS. A good example of these kind of risks could be Hurricane storm in Finland which would be catastrophically but highly unlikely. Other example could be not to check that all the small invoices are paid in time which might happen more often in a large organization but the damage would be very low. [1, 2]

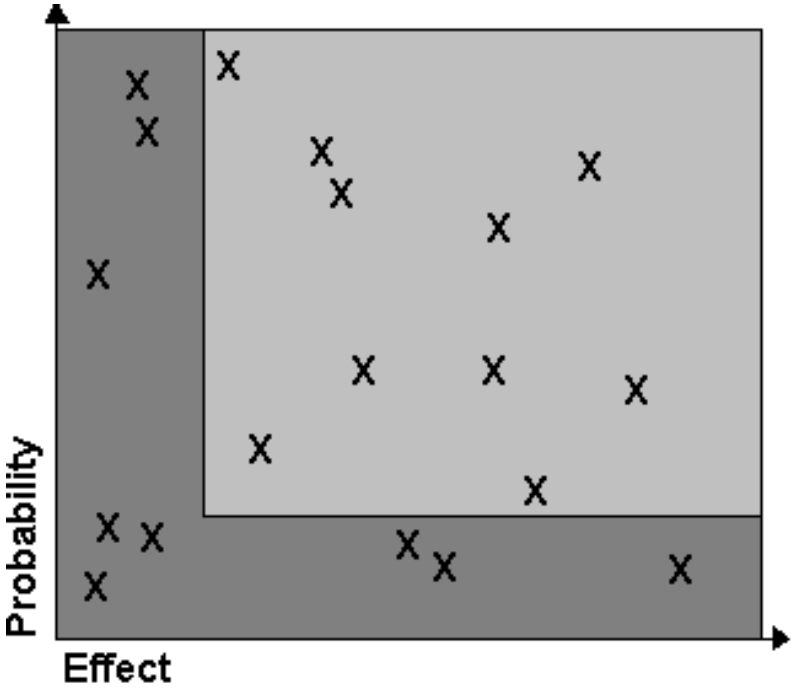

Figure 2: Risk assessment table light grey = applicable and dark grey = non-applicable risks [5]

Both of these two scenarios have their advantages. Sometimes some major risks have so small possibility that there is no need to take them under evaluation in risk management section even if acceptable level of risk is exceeded. On the other hand, it is simpler to calculate the risk levels and make conclusions based on the numbers. Both of these scenarios have one major disadvantage. How are the risks evaluated? How it is decided what is appropriate possibility or effect to certain risk? [1, 5]

As an example of the calculating the level of the risk could be classical hard drive example. In organization, there is a hard drive that is used to store customer data. Data is inserted to hard drive manually from paper form and it took two man

months to do the job. The specific hard drive is known to break during first five years with possibility of 50 percent. If man month is worth 3000 € to company and new hard drive costs 100 € the average level of risk is (2*3000€ +100€) * 0,5/5 = 610 €. Although result was gotten, it is not very accurate. For example, what is the value of the effectiveness lost when customer data is not available? [5]

When evaluating the risks there are usually very many different attributes that need to be taken under consideration. Usually the material effects are easy to calculate but the other ones are hard to measure. The calculations about the level of the risk are also used in management section.

MANAGE THE RISK

After the risk assessment is done, the next step in ISMS is risk management. This process involves prioritising, evaluating1 and (implementing)2 controls and actions to manage the risks defined in assessment section. Usually it is not practical to eliminate all the risks that were listed in risk assessment section. Usually the rule of using 'least-cost' method with implementing the 'most appropriate' controls to reduce the risks at the level defined in information security policy with 'minimal adverse impact' to organization is appropriate approach. [7]

1 The next step of ISMS concentrates especially on risks handling with controls [1, 3]
2 The implementing is formally done in the next phase of ISMS ("DO"-phase) [1]

When risk management is started, there are at least six different approaches to reduce the risk levels to acceptable level. These different approaches are described in Table 2. [7]

Table 2:

Assumption	Either to implement controls that reduce the risk to the acceptable level or just continue working as before without any actions.
Avoidance	Eliminate risks by eliminating the cause of the risk or the source of the threat.
Limitation	Reduce the level of the risk by minimizing the negative effect risk has to its vulnerability. For example support, prevention and detection
Planning	Make plans to manage the possible risks by using controls to reduce the level of the risk.
Transition	Transfer the risk to somewhere else. By doing this minimize the effect of the risk. Example insurances.
Research	Define and implement a research plan to acknowledge and correct the vulnerabilities that cause the risks.

Choosing the appropriate approach to risks that are defined applicable risks in risk assessment section is sometimes very difficult. In Figure 6 there is a flowchart that presents the path of the threat to the actual risk. There are four properties that need to be fulfilled. Eliminating any of these four properties will neutralize the risk. One approach could be going through this flowchart and make the decision on which stage the risk is eliminated based on the 'least-cost'- principle. Sometimes more than one threat can be neutralized with one countermeasure. If more than one risk is eliminated it has to be taken under evaluation when calculating the cost of risk neutralization. [3, 7]

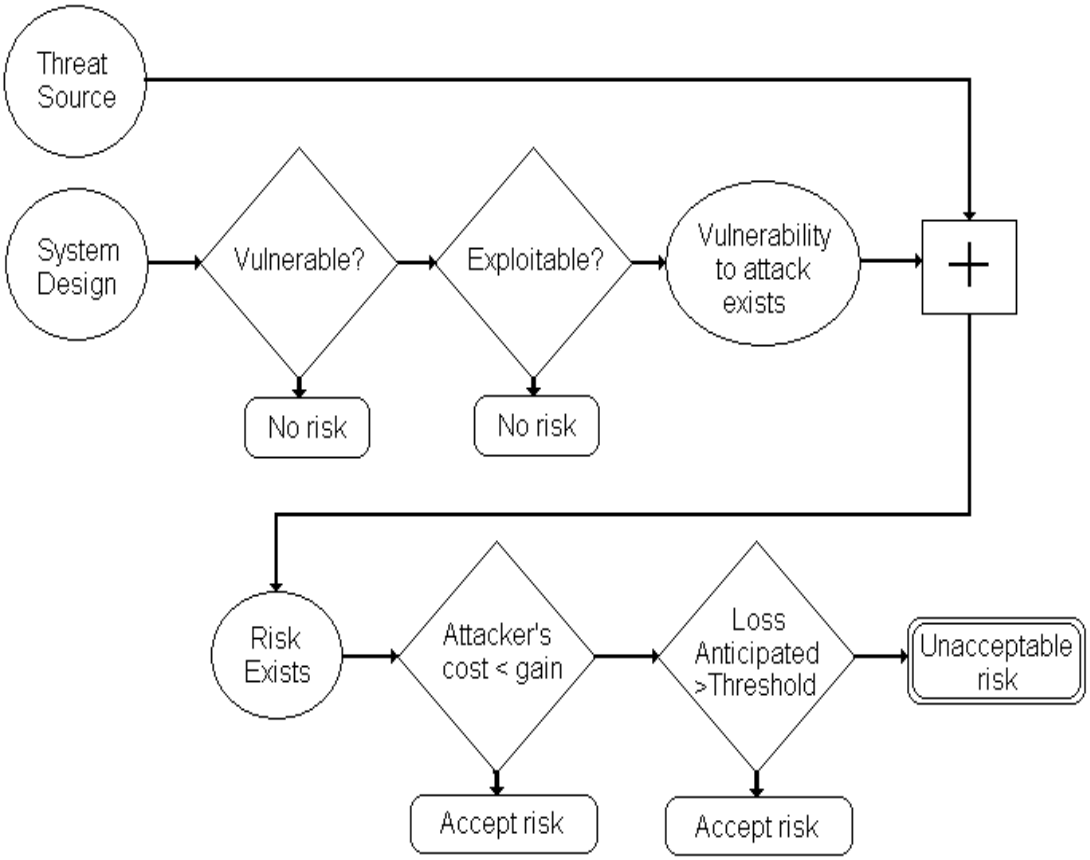

Figure 3: Risk management flowchart [7]

Managing the risk and the next step of ISMS 'Select control objectives and controls' are slightly overlapping because they both focus on what to do with the risks. A good separation of these two would be that in the 'controls'-chapter controls will be chosen to make sure that the threats are properly dealt with and managing the risk chapter tries to eliminate as many of these threats as possible. [1, 2, 3, 7]

Select control objectives and controls

Selecting controls and objectives that are controlled is a field that BS 7799 does not offer a simple solution. The first step to selecting controls has been done when security requirements have been chosen. The risks that have been defined in the risk assessment need usually controls. These controls can help reduce the risks to the acceptable level. This acceptable level of risks should be defined in the scope of ISMS. [2]

There are two basic models that are introduced here. The first one is classification of controls introduced in BS 7799 and the second one is a wayIUG (Internet User Group) introduces in their ISO 17799 journals. [2, 3, 4]

The model introduced by BS 7799 offers a solution where risks (control objectives) and their controls are classified to two different categories. The first one is legislative point of view. The controls that are protecting intellectual property rights or safeguarding organizational records or protecting data and privacy of personal information are considered legislative controls. The other control criterion is controls considered common best practice for information security. These controls include documents of information security policy, allocation of information security responsibilities, information security education and training, reporting security incidents and business continuity management. There is a list of possible control objectives in BS 7799. The list has 127 different objectives that might need controlling. This list is usually overall and most of the objectives might not be suitable to be used in an exact way although this list gives a good checklist when examining the organizations safety. Usually these controls have to be altered that they would fit the organization that they are used for.

When these controls are rewritten there has to remember that the objective of the control is not changed when the control statement is altered. [2, 3]

The other possibility to select controls is defined by IUG. In IUG's model, the controls can be categorized under four different categories. In this model, the categorization is clearer than in the model, BS 7799 represents. The first category is technology-based controls. These might be for example controls ensuring that the firewall or emergency power is working correctly. The second one is procedural controls. These controls might include for example the update procedures of the firewall and business software. How to make sure that the versions of software are updated on regular basis? The third one is personnel controls. How to make sure that the key personnel have the latest necessary skills to do their jobs in a way that the information security is not compromised.

The last one is physical controls, which is not the same than technology. Physical controls can be for example ways to make sure that the doors that need to be closed are closed. As for possible controls IUG point of view does not offer anything new to the view presented by BS 7799. The controls can bechosen beforehand from the 127 controls presented in BS 7799 or some other similar lists can be used. In Table 4, there are examples of the possible controls of the different categories objectives. [8]

As a summary of the control selection part can be said that the ISMS procedure does not offer a simple solution to this area. Perhaps the reason for this is that the controls used in different organizations can vary a lot. The classification of the controls is important because it is crucial to make sure that all the objectives that need controlling are controlled. The strength of the method IUG present is the clear classification of the controls that are needed versus the broader classification offered in BS 7799.

Table 3: Example of objectives and their controls [10]

Category	Objective	Control
Technology	Firewall as a product	Firewall is tested once in month. Firewall has a remote info panel that show the current state of the firewall.
Procedural	Updating firewall rules	Report from administrator to information security manager if firewall reconfigured. Log of possible changes.
Personnel	Skills of the administrator of the firewall	Possible tests from the managers or outside evaluators to key personnel.
Physical	Restricting physical access to firewall	Detector in the door that signals if the door is open. A log of door use is kept if the door uses electronic lock.

Prepare statement of applicability

The final step in ISMS planning phase is write a statement of applicability. This statement is a conclusion of what was decided in control selection phase. Statement of applicability should hold the information about the controls that were chosen and why they were chosen. In addition, the controls that were not chosen should be included to this document. For the controls that were not chosen there has to be some sort of explanations. [1, 3]

REFERENCES

[1]. Dr. David F. C. Brewer, ISO 17799 summary, Gamma Secure Systems Limited, 2004, White paper, Available at: http://www.gammassl.co.uk/bs7799/, Referenced June 4, 2004
[2]. Anonymous (Committee BDD/2), Information security management, BS 77991:1998 Code of practice for information security management, 1998, British standard
[3]. Anonymous (Committee BDD/2), Information security management, BS 7799-2:1999 Specification for information security management systems, 1999, British standard

[4]. David Bremer, Spotlight on incidents, ISMS Journal issue 2(Angelika Plate), ISMS International User Group Ltd, February 2003, Journal
[5]. J. Kontio, The Riskit Method for Software Risk Management, version 1.00, CS-TR-3782, University of Maryland. College Park MD, 1997, Technical Report Available at: http://www.soberit.hut.fi/~jkontio/, Referenced June 12, 2004
[6]. Anonymous (University of Florida computer science division), Information Technology Security Policy. University of Florida, UF Office of Information Technology, 2003, Web publication, Available at: http://www.it.ufl.edu/policies/security/, Referenced June 28, 2004
[7]. Gary Stoneburner, Alice Goguen, and Alexis Feringa, Risk Management Guide for Information Technology Systems - Recommendations of the National Institute of Standards and Technology, the National Institute of Standards and Technology, 2002, NIST special publications, Available at: http://csrc.nist.gov/publications/nistpubs/, Referenced July 8, 2004
[8]. David Bremer and Angelika Plate, Tao Zen practice and the art of holistic balanced, ISMS Journal issue 2(Angelika Plate), ISMS International User Group Ltd, February 2003, Journal