Global Information Assurance Certification Paper

Development of a Graded Baseline Security System

GIAC Security Essentials
Certification (GSEC)
Practical Assignment
Version 1.4b

Option 1 - Research on Topics
in Information Security

Submitted by: Raimo Peterson
Submitted: Oct. 04,2004

1 Table of Contents

2 Abstract

This paper describes the development process of a graded baseline security system for an organization or company, and compares it with other, non-graded and non-baseline approaches. It provides a generic view of techniques and considerations so as to form a structure into the company's security management. It provides depth into the benefits of information classification as well as the usage of graded baseline security systems over the non-graded baseline protection. This paper analyses the advantages and disadvantages of different possibilities, options and parameters, which must be specified during the development process. The whole development process is divided into 2 subtasks: development of classification model and the principle of assigning safeguards to the security classes. In order to illustrate theory with examples, this paper compares and analyses different existing baseline security systems.

This paper does not cover the development of safeguard catalogues for the security system – this may be consideration for further research. There will also be no focus on the roles and responsibilities of a company in which there will be relevance to the development process of the security system.

3 Introduction

Today, most companies use Information Technology to support their business processes. Some companies depend more on Information Technology than others, in which they inevitably pay more attention to Information Security as well. Within the evolution of a company, there will come a point whereby structured and systematic approaches to information security issues will be indispensable. There are many possibilities to bring structure into information security in which decisions are made by the upper management. One possible way is to establish a company wide Baseline Security System (BLSS). Although the development of a BLSS is resource consuming, it is easy to use once defined.

ISO/IEC TR 13335, a widely accepted international security guideline states that before starting any risk analysis activities, a company should have a strategy for risk analysis written into a corporate IT security policy. ISO/IEC TR 13335-3, chapter 8 lists four of the following different types of approaches for risk analysis:

- Baseline Approach
- Informal Approach
- Detailed Risk Analysis
- Combined Approach

According to the baseline approach, the whole security process (including risk analysis and the selection of safeguards) will be worked through only once in the development phase of BLSS. Subsequently, by applying similar safeguards to other information systems, a similar security level is expected. The major advantage and disadvantage of the baseline approach is as follows:

Advantage: The most cost and resource effective approach out of the four. In depth security know-how is not required to apply the BLSS on an information system.

Disadvantage: Usually intended for certain security levels, most often for the medium level. This baseline approach cannot be used for information systems, as it requires higher-level security than that of what the BLSS is developed to provide. As for information systems which require a lower level of security, defined baseline safeguards might be too expensive to apply.

Initially, the idea of this paper was to find a workaround solution for the above mentioned disadvantage. However, this research paper is extra comprehensive in a sense that it provides guidelines for the development of a BLSS, in which it includes a workaround solution for the major disadvantage mentioned above and yet remains cost effective compared to other approaches. Additionally, it provides deep consideration to the individual profile of a company.

Before starting with the development of a company's own BLSS, it makes sense to check if any already existing BLSS can be used. There has been development and publicity of international, national and organizational baseline security standards, as well as manuals and safeguard catalogues over the last few years. The following are some examples:

- German BSI, IT Baseline Protection Manual.
- ISO/IEC 17799 Code of practice for information security management (according to headline this is information security management standard, but from content it has similarities with baseline protection standard)
- U.S. DoE Classified Systems Security Manual

After the evaluation of the already existing and available BLSSs, it could be the case that they are unsuitable since most of them don't provide graded security or they don't meet the company's profile. Therefore, it would be necessary to develop a new graded BLSS to suit a specific company's profile.

The development of a graded BLSS has 2 major subtasks:

- The definition of a Classification Model for information systems (see chapter 4)
- The assignment of safeguards to each security class of the classification model (see chapter 5)

4 Classification Model

The information and information systems classification model of graded BLSS must meet the company's requirements. Some companies have their business processes highly integrated with the information systems, while other companies' information systems are playing only a supportive role. Therefore, the requirements for Security Objectives (SOs) and the classification model of information systems will be different for these companies. Decisions about the suitability of a classification model can only be done by the management level of information owner or a custodian, who would be familiar with the values of the information and possible impacts to the business if security requirements are not met.

4.1 Security Objectives (SOs)

In some developments, the information systems' classification granularity is limited to one general SO with three or four levels. Most often this general objective is similar to the confidentiality and classification levels are something similar to unclassified, confidential, secret and top secret.

It is possible that at the beginning, this one-dimensional granularity is acceptable for a small company, but larger organizations who have large variety of different information systems, and who are more dependent on information security, require higher classification granularity.

More often a classification model with 3 SOs is used. These three objectives are defined in different international, national and organizational sources in different ways. According to ISO/IEC international standard 17799:

- **Confidentiality** is ensuring that information is accessible only to those authorized to have access.
- **Integrity** is safeguarding the accuracy and completeness of information and processing methods.
- **Availability** is ensuring that authorized users have access to information and associated assets when required.

First, the requirements for the granularity of the information system's classification model must be considered. If the usage of the above mentioned 3 SOs is not acceptable granularity, or these SOs do not match with the profile of a given company, then different SOs must be used for the classification model. The accuracy of the whole BLSS will depend on the classification granularity. If higher accuracy is needed, classification model must have more SOs and SOs must have more levels. One possibility to achieve a better granularity is to split one or more SOs into 2 sub-objectives, like it is done with SO of availability in example 2 on page 5.

The introduction of new SOs is bound to costs, time, money and resources. Upon defining safeguards for the information system classes (chapter 5.2), it will be clear that theoretically the needed number of sets of safeguards will increase exponentially by defining new SOs with new levels. The SOs for the classification model should be very carefully defined as later changes are very expensive to contend with.

Some sample publications with more than 3 SOs are:

1) Safeguards in ISO/IEC TR 13335-4, chapter 10 are grouped according to six SOs:
   - Confidentiality
   - Integrity
   - Availability
   - **Accountability** is the property that ensures that the actions of an entity may be traced uniquely to the entity
   - **Authenticity** is the property that ensures that the entity of a subject or resource is the one claimed. Authenticity applies to the entities such as users, processes, systems and information.
   - **Reliability** is the property of consistent intended behavior and results.

In addition, ISO/IEC TR 13335-5 chapter 13.11 focuses on the SO of Non-Repudiation from the viewpoint of network security. **Non-Repudiation** is assurance that the sender of data is provided with proof of delivery and the

recipient is provided with proof of the sender's identity. Therefore, neither can later deny having processed the data.

2) The Estonian public sector three-level BLSS has granularity of 4 SOs with four levels for each SO. This graded BLSS uses only 2 from the common SOs: confidentiality and integrity. The third commonly used SO availability is split into two sub-objectives:

   - **Time Criticality of Data** expresses the maximum time in which data has to be available after request.
   - **Severity of Consequences of Delay** expresses the possible losses should data not be available on time.

The breaking up of availability provides more accurate classification in case of state owned public sector information.

3) NIST uses in special publication 800-33 in addition to confidentiality, integrity and availability (sometimes also called "big three" or CIA), accountability and assurance. **Assurance** is the requirement which makes sure that the targets of other SOs have been adequately met.

4) HIPAA, focuses on **Privacy**. Sometimes privacy is seen under confidentiality, but in the field of healthcare as it makes sense to have a separate SO for this requirement. Privacy is an individual's right to have control over the usage of their personal information. If there is a special privacy SO defined, then most commonly the term "confidentiality" will be used in the context of business information.

By defining the company specific classification model for a graded BLSS, it is recommended to have confidentiality, integrity and availability as minimum granularity of the classification model. If necessary, additional SOs from the examples above or from other sources must be introduced in accordance to the given company's profile.

Before finalizing the SOs used in a company's classification model, existing binding policies, rules, regulations and laws of the government must be checked.

4.2 Levels of Potential Impact (LoPIs)

After defining the SOs, it is necessary to define the number of levels within each SO. The Level of Potential Impact (LoPI) is a parameter of the classification model, which indicates the potential impact (or harm) to the company, if requirements for specific SOs are not met.

Beside of the number of SOs, the accuracy of overall protection depends on the number of LoPIs. If the granularity of the classification model is too low, then later by classifying a specific information system, it may become over- or underclassified. Underclassification is a dangerous security leak because safeguards applied to the information system will not provide the required security level. Overclassification is just wasting of resources, because too many

safeguards will be used for protection of a specific information system. Better managed use of these resources would provide better overall security.

On the other hand, introducing too many security levels will increase the complexity of the whole BLSS. Please refer to chapter 5.2 for the instructions on how to map safeguards to the security classes and the influences of the classification granularity has over the selection of safeguards.

Basically, it is possible to proceed in accordance to one of the following options:

- To specify the same number of levels for each SO (e.g. low, medium and high for each of confidentiality, integrity and availability). This option will be named as flat distribution of LoPIs.
- To analyze each SO separately and to decide how many levels are needed for the SO for a given company (e.g. 6 levels for confidentiality, 3 for integrity, 2 for availability, 3 for accountability). This option will be named as weighted distribution of LoPIs.

Total number of different security classes will be calculated by multiplying the number of LoPIs for each SO. The following three examples will give an overview of which impact the granularity has to the total number of security classes.

- For the first example above (3 objectives, 3 levels for each SO) will give 3 x 3 x 3 = 27 security classes.
- For the Second example above (6 levels for confidentiality and 3 for integrity, 2 for availability, 3 for accountability) we will get 6 x 3 x 2 x 3 = 108 security classes
- A classification model with 5 SOs and 5 levels for each objective will give 5 x 5 x 5 x 5 x 5 = 3125 security classes.

Theoretically it is necessary to map one set of safeguards to each security class. If it would be necessary to develop 3125 sets of safeguards, like in the example above, one may have a question concerning the validity of the initial idea of baseline security – cost effectiveness. Would it be cheaper to perform a detailed risk analysis for all information systems instead? The answer to this question will be clearer after reading chapter 5.2.3, where synergies and optimization possibilities are covered.

As a general rule, if the organization profile is “confidentiality weighted” or “availability weighted”, the classification model should have more LoPIs for these objectives defined. This weighted approach with different numbers of LoPIs for each SO enables a better company specific accuracy of the whole BLSS with lower costs.

Last, but not least is to be careful with the terminology in different sources. FIPS 199 uses the term “Potential Impact”, DOE M 471.2-2 uses the term “Level of Concern” and “Sensitivity” ISO/IEC TR 13335-5 has a different view of classification – network view and defines the classification levels as “Trust

Relationship" levels. Estonian public sector three-level BLSS uses the terminology of "Requirement level" for SO.

4.3 Classification Rules for each LoPI

Classification of information and information systems must be performed by the information owner, often called a custodian. Often there are many different custodians within the organization. LoPIs like low, medium and high or even public, confidential, secret and top secret can be interpreted differently by different persons. Therefore, the classification model is objective and useful only if precise company specific rules are given for each LoPI of each Objective. These rules must map with other binding guidelines for the organization.

Some examples from already used references:

1) FIPS 199 gives a very general definition for three LoPIs, which are same for each SO:

- The potential impact is LOW if the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
- The potential impact is MODERATE if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
- The potential impact is HIGH if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

This very generic definition doesn't help a custodian much to make decisions in terms of which LoPI should be specified for information. Basically instead of deciding between low, moderate and high, a custodian has to choose between limited adverse effects, serious adverse effects and severe or catastrophic adverse effects.

2) DOE M 471.2-2 gives a more precise description between low, medium and high Levels of Concern (similar to LoPI in this paper). Each SO has its own description for each three Levels of Concern. The following example (excerpt from DOE M 471.2-2) shows the description of Levels of Concern for the SO availability only:

Level of Concern	Qualifiers
High	Information must always be available upon request, with no tolerance for delay; or loss of life might result from loss of availability; or loss of availability will have an adverse effect on national-level interests; or loss of availability will have an adverse effect on confidentiality
Medium	Information must be readily available with minimum tolerance for delay; or bodily injury might result from loss of availability; or loss of availability will have an adverse effect on organizational-level interests.
Low	Information must be available with flexible tolerance for delay.

Table 1: Description of Levels of Concerns in DOE M 471.2-2

Note: In this context, “High – no tolerance for delay” means no delay; “Medium – minimum tolerance for delay” means a delay of seconds to hours; and “Low – flexible tolerance for delay.” means a delay of days to weeks.

It is possible that first at describing the LoPIs for each SO, it will become visible that the number of initially defined LoPIs must be increased or decreased.

The generic recommendations for the description of LoPIs are:

- To get maximum accuracy and cost effectiveness, give separate LoPI descriptions for each SO.
- To describe the LoPIs as detailed as possible and at the same time as generic as necessary, considering the profile of your organization. The more detailed the description, the better will be the accuracy of the classification of information systems.
- Consider that the classification of information systems will not be done by security professionals. If necessary, a separate guideline must be published, which gives specific classification rules for the different types of information systems in the organization (refer to NIST Special Publication 800-60).
- If necessary, don’t hesitate to change the granularity of classification model, by adding or removing LoPIs or even changing the number of SOs.

Security Class of an information system is defined if the information system has got a LoPI value for every SO of the classification model.

By specifying the LoPIs it is recommended to number them starting from zero, and not to name them like in previous examples (Low, Medium, High). If the LoPIs are numbered, it is much easier to refer to a specific security class. Therefore one capital letter (or a capital letter and a small letter) will be assigned

to each SO. For example: C – for confidentiality, I - for integrity and A for availability. LoPIs are numbered from 0 upwards, where 0 is the lowest level and means that there are no requirements for the SO and subsequently there can not be negative impact associated with this SO. Security class will be written like **C3I2A1**, which tells us that for one specific information system confidentiality LoPI has value 3, integrity LoPI has value 2 and availability LoPI has value 1.

4.4 Applying the Classification Model

By classifying an information system according to a classification model of graded BLSS, it becomes visible that even if all security classes (combinations of all SOs and LoPIs) are theoretically possible, some of them don't make sense. The reason for this is that certain inter-dependencies exist between different SOs (refer NIST 800-33)

Confidentiality and integrity are interdependent. On loss of the confidentiality, there shouldn't be high expectations that integrity still exists.

The other way around – on loss of integrity, we shouldn't expect that the confidentiality mechanisms are still valid.

By defining the LoPI value for confidentiality and integrity, they shouldn't be very different for the same information system. As a rule of thumb, no more than one level of difference between confidentiality and integrity should be specified if the classification model has granularity of three or four LoPIs for both SOs.

Furthermore, availability is depending on confidentiality and integrity. A high LoPI value specified for availability of an information system requires a high LoPI value for confidentiality and integrity of the same information system.

The defined classification model can be applied for information and for information systems. If information system comprises information from different security classes, the security class of Information system will get the highest LoPI values of all information for each SO. Example:

Information	Security Class
Database 1	**C1I2A2**
Database 2	**C2I3A1**
Database 3	**C2I2A2**
Information system running databases 1, 2 and 3	**C2I3A2**

Table 2: Defining the security class of the information system.

5 Selection of Safeguards

Risk analysis and the selection of safeguards are the most resource consuming tasks in development of a graded BLSS. One of the reasons is that these tasks require formal risk analysis, which is resource consuming. On the other hand, this must be done only once, and that is in the development phase of BLSS. To reduce the risks to an acceptable level (defined baseline level), a set of safeguards will be specified. This procedure is similar to the approach of a detailed risk analysis defined in ISO/IEC TR 13335-3 chapter 9.3.

The defined set of safeguards will be reusable for systems with similar security requirements. Theoretically, the risk analysis and the selection of safeguards must be made once for each security class, so that each security class will have its own set of safeguards. All safeguards for all security classes form a **safeguard catalogue** of the BLSS. To achieve the baseline level security for information system, **all** safeguards defined for specific security class must be implemented without any further analysis. The process of specifying the needed safeguards from the safeguard catalogue should be automatized. Simple software helps to avoid human mistakes and to force system administrators to comply to rules.

5.1 Evaluation of existing Safeguard Catalogues

Apart from the fact that effective safeguards are changing quickly, there is also the issue of keeping already defined safeguard catalogues up to date which is resource consuming. In most cases, the company doesn't have enough resources to develop its own baseline safeguards catalogue from scratch. In this case, it makes sense to find a suitable, already existing safeguard catalogue and to adapt it for the needs of the company and the already defined classification model of graded BLSS.

To evaluate the existing safeguard catalogues, first the requirements for the base safeguard catalogue must be defined. Some aspects to consider are:

- A safeguard catalogue should be based on similar SOs of the classification model of the company's BLSS.
- Baseline security level of a safeguard catalogue should be similar to security levels of the company's BLSS
- The number of specified safeguards should be big enough and the safeguards should be specified in detail (granularity requirement).

Before adapting any existing safeguard catalogue, author rights and legal aspects must be clarified.

5.2 Mapping the Safeguards to Security Classes

Graded BLSS is completely defined, if there is possible to assign one pre-defined set of safeguards to each security class without any additional analysis.

5.2.1 Vertical Approach

One approach to achieve the target is to assign a set of safeguards to each LoPI of each SO. To distinguish this approach from others, it will be referred to as a vertical approach in this paper. It is advisable to set up the vertical approach so that the safeguards for higher LoPIs include all safeguards of lower LoPIs plus some additional ones. This layered approach enables cost effective upgrades if there should be reclassifications to a higher security class at a later stage. In this case only some additional safeguards, which correspond to the new, higher LoPI must be implemented. Example in Table 3 illustrates the principle of vertical mapping of safeguards.

Control Area	LoPI for Confidentiality						LoPI for Integrity			LoPI for Availability			Safe-guards for Class **C5I2A2**
	C1	C2	C3	C4	C5	C6	I1	I2	I3	A1	A2	A3	
Alternate Power Source										APS-1	APS-2	APS-3	APS-2
Audit Capability	AUD-1	AUD2	AUD3	AUD-4	AUD-4	AUD-5	AUD-1	AUD-2	AUD-3				AUD-4
Backup and Restoration							BRD-1	BRD-2	BRD-3	BRD-1	BRD-2	BRD-3	BRD-2
Changes to Data							CD-1	CD-1	CD-2				CD-1
Communications	COM-1	COM-1	COM-1	COM-1	COM-1	COM-1	COM-1	COM-1	COM-2				COM-1
Configuration Management	CM-1	CM-1	CM-2	CM-3	CM-3	CM-3	CM-1	CM-2	CM-3				CM-3
Disaster Recovery Planning										DRP-1	DRP-2	DRP-3	DRP-2
Independent Validation				IVV-1	IVV-1	IVV-2							IVV-1
Resource Access Control		RAC-1	RAC-2	RAC-3	RAC-3	RAC-3							RAC-3
Resource Utilization		RU-1	RU-2	RU-2	RU-2	RU-2							RU-2
Security Documentation	SD-1	SD-1	SD-1	SD-2	SD-2	SD-2							SD-2
Separation of Functions			SF-1	SF-1	SF-1	SF-1							SF-1
System Recovery	SR-1	SR-1	SR-1	SR-2	SR-2	SR-2							SR-2
Security Support Structure	SSS-1	SSS-1	SSS-2	SSS-3	SSS-3	SSS-3	SSS-1	SSS-2	SSS-3	SSS-1	SSS-2	SSS-3	SSS-3
Security Testing	ST-1	ST-2	ST-2	ST-3	ST-3	ST-3	ST-1	ST-2	ST-3				ST-3
Trusted Path					TP-1	TP-1							TP-1

Table 3: Vertical mapping of safeguards.

Note: The fictive example in Table 3 doesn't pretend to be consistent nor complete. The control areas and safeguards in this example are taken (with some changes) from DOE M 471.2-2, terminology and principle is changed to match with this document.

The example in Table 3 shows the idea of mapping the safeguards to security classes of vertical approach. The classification model used in the example has 6 LoPIs for confidentiality and 3 LoPIs for integrity and availability. Safeguards in this example are from a safeguard catalogue which is built in a layered way. Each LoPI of each SO has been assigned a set of safeguards from a safeguard catalogue of graded BLSS. The last column shows the highest required set of safeguards out of each SO for the sample security class **C5I2A2** (This procedure should be automatized). To get the baseline security for an information system in this class, all the safeguards in the last column of Table 3 must be implemented.

Some safeguards used within a vertical approach have positive or negative influences to many SOs. It becomes a problem if safeguards intended for one

specific SO may have a negative influence to other SOs. Safeguards for a high confidentiality (for example strong authentication and encryption) may have a negative impact for availability. The problem becomes most critical for the information systems for which a very high LoPI value for both of confidentiality and availability are defined. After implementing all the required baseline safeguards for the security class, it can happen that confidentiality safeguards have reduced the system availability so that even after implementing all availability safeguards, the required availability level is not achieved.

5.2.2 Horizontal Approach

Other approach of mapping safeguards to security classes is the definition of an own set of safeguards for each security class. This will be referred to as a horizontal approach in this paper. A horizontal approach doesn't have the safeguard influence problem, because a risk analysis is performed for each security class.

Since the classification model of a graded BLSS may define many thousands of security classes (refer chapter 4.2), some kind of optimization is necessary, otherwise the effort for risk analysis of each class will be too high.

5.2.3 Optimized Approach

One example for the optimized mapping of safeguards to a security class is the Estonian public sector three-level BLSS. The classification model of this graded BLSS has 4 SOs (see chapter 4.1, example 2): Confidentiality (C), Integrity (I), Time Criticality of Data (T) and Severity of Consequences of Delay (S). Each SO has 4 LoPIs defined (0, 1, 2 and 3), so the total number of security classes is 4 x 4 x 4 x 4 = 256. Instead of developing safeguard sets for 256 security classes, a new property - **security level** (high, low or medium) is assigned to each security class according to the following rules (which has also some exceptions):

- If one or more LoPIs in security class have value 3, then the security level is high (H)
- If one or more LoPIs in security class have value 2, then the security level is medium (M)

Table 4 (from the Estonian public sector three-level BLSS, slightly adapted) shows the security levels for all 256 security classes.

This BLSS defines one set of safeguards for security level L (must be always implemented) and one set of safeguards for security level M (must be implemented in addition to level L safeguards).

		S0				S1				S2				S3			
		T0	T1	T2	T3	T0	T1	T2	T3	T0	T1	T2	T3	T0	T1	T2	T3
I0	C0	L	L	L	H	L	L	M	H	M	M	M	H	H	H	H	H
	C1	L	L	M	H	L	L	M	H	M	M	M	H	H	H	H	H
	C2	M	M	M	H	M	M	M	H	M	M	M	H	H	H	H	H
	C3	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H
I1	C0	L	L	M	H	L	L	M	H	M	M	M	H	H	H	H	H
	C1	L	L	M	H	L	M	M	H	M	M	M	H	H	H	H	H
	C2	M	M	M	H	M	M	M	H	M	M	M	H	H	H	H	H
	C3	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H
I2	C0	L	M	M	H	M	M	M	H	M	M	M	H	H	H	H	H
	C1	M	M	M	H	M	M	M	H	M	M	M	H	H	H	H	H
	C2	M	M	M	H	M	M	M	H	M	M	M	H	H	H	H	H
	C3	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H
I3	C0	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H
	C1	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H
	C2	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H
	C3	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H

Table 4: Mapping of Security Levels to Security Classes.

For security level H, five additional sets of safeguards are defined:

- **Generic set of safeguards**, which must be implemented always for the security level H
- **Safeguards for C3**, which must be implemented only if confidentiality has LoPI value 3
- **Safeguards for I3**, which must be implemented only if integrity has LoPI value 3
- **Safeguards for T3**, which must be implemented only if time criticality of data has LoPI value 3
- **Safeguards for S3**, which must be implemented only if severity of consequences of delay has LoPI value 3

As seen from this example, the used optimization allows the creation and maintenance of only 7 sets of safeguards instead of 256. Of course, after this optimization, the initial granularity and also accuracy on the lower security levels is lost. That may cause overprotecting on lower levels. The initial granularity still exists on high security level, where the implementation of safeguards is most expensive. The principle of this optimized approach can be used for any other graded BLSS with different classification models.

6 Conclusion and Recommendations

Developing a graded BLSS for a company is not only time and resource consuming, but also a challenging task. The following checklist gives an overview of important considerations during the development of a graded BLSS:

- Write down the company specific requirements for the graded BLSS. Consider the alternative solutions and if the overall security level of BLSS is acceptable.
- Work through available existing BLSSs, considering if some of them can be adapted for company use, and what kind of changes would be necessary.
- What is the desired accuracy of the BLSS? Is +/- 10% acceptable?
- What is the acceptable granularity of the classification model? Is the usage of CIA precise enough or must some additional SOs be added? How many levels are needed for each SO?
- Do all SOs have similar importance to the company or are some of them more important? Decide between the use of flat distribution or weighted distribution of LoPIs.
- Where to get safeguard catalogues? Is the development of company specific safeguard catalogues too expensive? What are the legal aspects to adapt an existing catalogue?
- How to map safeguards to security classes. How many different classes are there? Is it possible to define one set of safeguards for each security class? Should some optimization be performed? Is the SO inter-dependency fault of vertical approach acceptable?
- Define the update procedure of the security system.

7 References

ISO/IEC Technical Report 13335 “Information technology — Guidelines for the management of IT Security” 1996-2001

BSI, Germany “IT Baseline Protection Manual” 2003
http://www.bsi.de/gshb/english/etc/index.htm
http://www.bsi.de/english/fb/F14itbas_en.pdf

ISO/IEC International Standard 17799 “Information technology — Code of practice for information security management”

U.S. Department of Energy, Office of Security Affairs DOE M 471.2-2 “Classified information systems security manual” 1999

Infosüsteemide Kolmeastmelise Etalonturbe Süsteem ISKE.
(Information Systems’ Three-Level Baseline Security System), 2003
http://www2.cyber.ee/dokumendid/ISKEjuhend.pdf (in Estonian language)
http://www.riso.ee/en/it98eng/72.htm (only classification model in English)

NIST Special Publication 800-33 ” Underlying Technical Models for Information Technology Security” 2001
http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf

HIPAA “Health Insurance Reform: Security Standards; Final Rule”
http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/03-3877.pdf

HIPAA “Standards for Privacy of Individually Identifiable Health Information; Final Rule” http://www.hhs.gov/ocr/hipaa/privrulepd.pdf

Federal Information Processing Standards (FIPS) Publication 199 “Standards for Security Categorization of Federal Information and Information Systems” 2003
http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

NIST Special Publication Draft 800-53 “Recommended Security Controls for Federal Information Security Systems” 2003.
http://csrc.nist.gov/publications/drafts/SP800-53-Draft2nd.pdf

NIST Special Publication 800-60 “Guide for Mapping Types of Information and Information Systems to Security Categories” 2004.
http://csrc.nist.gov/publications/nistpubs/800-60/SP800-60V1-final.pdf
http://csrc.nist.gov/publications/nistpubs/800-60/SP800-60V2-final.pdf

P.H.Samwel, M.E.M.Spruit,” A practical approach to manage data communication security” 1999
http://www.cs.plu.edu/courses/CompSec/arts/sec1999.doc