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: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

Safety Assessments Methodologies and Application for the Deployment of Laptops in Production System Environments

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

Option 1 - Research on Topics
in Information Security

Submitted by: Gerd Els
Location: London

© SANS Institute 2005, Author retains full rights.

Table of Contents

List of Figures

© SANS Institute 2005, Author retains full rights.

Abstract/Summary

An overview of some existing safety and risk assessment methodologies is given. The common way to perform a safety assessment is presented. The common risk definition as a two dimensional is pointed out. The application of a simple qualitative safety assessment method is shown in form of a case study regarding the deployment of laptops in production system environments. After the initial hazard analysis and the following determination of the risk some measures are presented in terms of policy statements. The policy statements could be used to design a safety policy for the deployment of laptops in production system environments and tailored for other cases. It is shown in which way these measures are affecting the severity, the frequency, and finally the risk for the identified hazards. As a result of the presented safety analysis it was found that only a defense in-depth strategy considering functional and organizational measures for the laptop as well as for the production system can lead to an acceptable risk reduction.

Introduction

It is the daily business of an IT-security professional to think about possible hazards and the related risks when looking at his systems. For the case he identifies a risk related to a hazard he will normally try to minimize the risk. He will possibly introduce the easy and cheap measures which are able to reduce the identified risk directly by himself. For the difficult and expensive measures he has to discuss them with the appropriate management level which will weight up the enhanced security introduced by and the costs of these measures.

At this point the IT-security professional will have to present the risks and the effects of the proposed measures on the risks in a way that the management can understand them and is able to make the necessary and right decision. It is therefore important that the hazards and the related risks are determined in a systematic way. A safety assessment or risk assessment will lead to such a systematic identification of existing hazards and the related risks. IT-security professionals should be able to use and apply this toolbox in their daily business.

The paper will therefore give an overview of existing methodologies and the different classification schemes for the risk. It will also show in form of a case study how a safety assessment is working. Furthermore, it will be shown how it can help to find appropriate measures to reduce the risks related to identified hazards.

Safety and Risk Assessment Methodologies

There are several descriptions and methodologies how a risk or safety assessment can be performed systematically. Besides of international standards there are organisations for which safety and security are very important and

© SANS Institute 2005 Author retains full rights.

which are therefore publishing their own methodologies for risk or safety assessments. In the following an overview of some existing standards and methodologies is given and described shortly. A special focus is later laid on organisations related to airspace industry. The list does certainly not claim to be complete.

ISO/IEC 17799 Information technology - Code of practice for information security management [1]

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) are publishing the standard ISO/IEC 17799. The standard was originally developed by the British Standards Institution (BSI) as the British standard BS 7799. The BS 7799 was later adopted by ISO/IEC to the ISO/IEC 17799 standard.

As the title of the standard implicates it is a code of practice. It gives within 12 chapters recommendations for the initiation, implementation and maintenance of security for IT-environments.

Just a rough overview about the meaning of a risk assessment is given in the introduction. According to the standard a risk assessment identifies the business harm and the realistic likelihood of a security failure to occure by considering the threats and the vulnerabilities.

MIL-STD-882D: Standard practice for system safety [2]

The MIL-STD-882D was developed by the Department of Defense of the United States of America. The document describes a standard practice how the safety of a system and the related risks can be evaluated. The system safety is here discussed with the focus on risks for mishaps.

The methodology can be summarized as follows: In a systematic hazard analysis the possible hazards are identified. The mishap risk for each hazard is then determined by assessing the severity and probability.

The severity of a possible mishap risk is categorised in four categories:

- I Catastrophic,
- II Critical,
- III Marginal, and
- IV Negligible.

The probability of a possible mishap risk is categorised in five levels:

- A Frequent,
- B Probable,
- C Occasional,
- D Remote, and
- E Improbable.

© SANS Institute 2005 Author retains full rights.

A matrix links the severity category and the probability level of an identified hazard to mishap risk assessment values. These mishap risk assessment values range between 1 and 20 and can be assigned to one of the four the mishap risk categories

- High (mishap risk assessment value between 1 and 5)
- Serious (mishap risk assessment value between 6 and 9),
- Medium (mishap risk assessment value between 10 and 17), or
- Low (mishap risk assessment value between 18 and 20).

When unacceptable mishap risks are identified they should be addressed by developing measures which are able for instance to mitigate, eliminate and reduce mishap risk to an acceptable level. A verification of the reduction as well as the acceptance of residual mishap risk by the appropriate authority is also demanded.

NASA

The National Aeronautics and Space Administration (NASA) of the United States of America is also a good source for standards related to safety issues.

To get a good and short introduction into risk assessment methodology and risk management at NASA organisation a presentation with the title “Risk Assessment and Management, Tools and Applications” is available on internet.[3] It is highlighted that a risk is a two dimensional quantity. The two dimensions are the likelihood or frequency in one dimension and the magnitude or severity in the other dimension. A quantitative as well as a qualitative approach to determine the risk in those two dimensions is presented. In the qualitative approach the frequency as well as the severity are categorised in three categories:

- Low
- Medium
- High.

The risk is categorised in four classes according to the combination of frequency and severity.

- High,
- Serious,
- Medium,
- Low.

A more detailed description of the NASA safety assessment methodology is given in the NASA Safety Manual.[4] This is a NASA Procedural Requirement (NPR) document with the number 8715.3. The manual gives an overview about safety issues in general. The NASA hazard assessment methodology is described herein in more detail. The proposed classification schemes for the probability of occurrence and the severity of consequence of an identified hazard are similar to MIL-STD-882 which was already described previously herein.

© SANS Institute 2005 Author retains full rights.

EUROCONTROL

EUROCONTROL is the European Organisation for the Safety of Air Navigation. The organisation published an introduction to a safety assessment methodology with the focus on air navigation systems.[5]
It describes a three step process for a safety assessment during the lifecycle of air navigation systems. Within the system definition phase a functional hazard analysis (FHA) is performed as the first step. The FHA determines the necessary safety level for the system. The FHA starts by specifying the functions of the system to be developed. Next, the system failure modes (such as loss or degradation of the functions) are identified. Finally, the potential hazards associated with these failure mode(s) are identified. For each potential hazard the risk is identified. The risk is defined as combination of the overall frequency of occurrence of a harmful effect induced by the hazard and the severity of that effect.[6]

In the design phase a so called preliminary system safety assessment (PSSA) is performed as second step. The PSSA will check whether the system architecture can achieve the safety level specified in the FHA. The third and last step is the system safety assessment (SSA) in the integration phase. The SSA will re-examine whether the system implementation will achieve an acceptable risk. The methodology using three steps during the life cycle of a system could certainly be generalised and should be applicable also for other systems than air navigation systems.

The guidance material which is provided proposes also risk classifications schemes. For instance a severity class scheme of five classes with a list of possible indicators to choose the appropriate class is provided in Reference [7]. In Reference [5] some examples are furthermore provided how a risk classification scheme can be set-up dependent on frequency and severity of the hazard.

A complete overview of all documents related to the safety assessment methodology can be found under Reference [8]. From this web site it is possible to download the different parts and chapters of the safety assessment methodology.

Federal Aviation Administration (FAA)

The Federal Aviation Administration (FAA) of the United States of America publishes some well written descriptions about their safety assessment methodology. An overview about safety and risk issues at FAA can by found under Reference [9]. To get an overview about system safety process Reference [10] can be recommended. A detailed description is given in the “FAA System Safety Handbook” [11] which provides “practices and guidelines for conducting system safety engineering and management”.

© SANS Institute 2005 Author retains full rights.

The risk is characterized by the severity and the likelihood of occurrence of a hazard. The FAA system safety handbook distinguishes between five classes of severity

- Catastrophic
- Hazardous
- Major
- Minor
- No Safety Effect,

four classes of likelihood:

- Probable
- Remote
- Extremely Remote
- Extremely Improbable,

and gives definitions for each.

The risk can be determined by a risk acceptability matrix which combines severity and likelihood. Dependent on the likelihood and the severity the three risk acceptance criteria

- High Risk
- Medium Risk
- Low Risk

are determined for the hazard.

Safety Assessment Methodologies- Summary

In the last chapter some risk and safety assessment methodologies were presented. The first step of a safety or risk assessment is to perform a systematic identification of possible hazards. After that, for each hazard the severity and also the frequency of occurrence are determined using defined classification schemes. According to the severity and frequency of occurrence the risk is determined using a two-dimensional matrix which links these two properties to the risk. The differences are mainly based on the different classification schemes used for the severity, probability, and risk.

Safety Assessment – A Case Study for the Deployment of Laptops in Production System Environments

This chapter will show how a safety assessment can be performed. This will be done in form of a case study. The case will focus on the deployment of laptops in production system environments.

Case Description

Let us assume the following situation: There is a company which runs an IT production system. It is essential for the company that this production system is highly available (24h a day and 7 days a week). It is furthermore necessary to

© SANS Institute 2005 Author retains full rights.

guarantee the integrity and the confidentiality of this network. A defense in-depth strategy was accomplished to the production system after a careful hazard analysis. To accomplish availability, integrity, and confidentiality the production system has limited, restricted, and well secured connections to the outside world.

The situation may now occur that the support personnel must connect sometimes a laptop to the production system for maintenance reasons. Let's assume for this case study that there is no other way than using laptops. In our example several persons have to use a laptop due to shift-work. They all must have administrator privileges on the laptop.

Due to the mobility of laptops, an enhanced risk level to hacker, virus, and worm attacks to laptops can be assumed. This can lead to an indirect risk for the production system to which the laptops has to be connected. To determine the risks for the production system a safety analysis has to be performed.

The goal is determine the associated risk and to give - if necessary - appropriate recommendations for risk reduction to the responsible management. The recommendations should lead to a policy for the deployment of laptops in the production system environment.

Safety Assessment Method

According to the overview on existing risk and safety assessment methodologies in the first chapter of this document the simple qualitative method proposed by Reference [3] was chosen to perform a safety assessment for the deployment of laptops in production system environments.
In the qualitative methodology the risk is expressed in terms of the frequency and the severity of a hazard. The frequency as well as the severity are categorised in the three categories:

- Low,
- Medium, and
- High.

The resulting risk is categorised in the four classes

- High,
- Serious,
- Medium, or
- Low.

The risk category is determined according to the combination of frequency and severity corresponding to the simple qualitative risk assessment matrix depicted in Figure 1.[3]

© SANS Institute 2005 Author retains full rights.

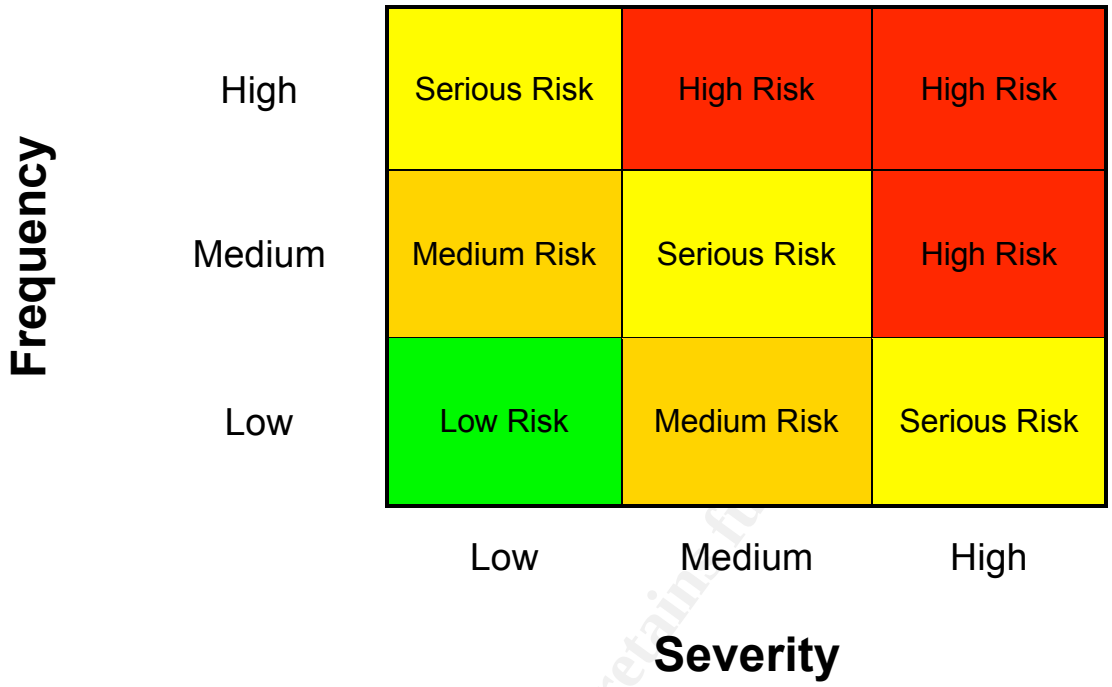

Figure 1: Qualitative risk assessment matrix.[3]

Hazard Identification

In the following a hazard identification will be presented for our case. The presented hazards are on a relatively high and general level. The goal here is to show how a safety assessment works and how appropriate measures can influence the risks of an identified hazard. A detailed hazard analysis is not in the scope of this work. The identified high level hazards are listed below.

Hazard 1: Remote attack

A remote access of the production system for the laptop can also be used to attack the production system in the way

- that a denial of service (availability) is achieved.
- that backdoors are established which could harm the confidentiality and integrity of the data on the production system.

Hazard 2: Direct attack

A laptop directly connected to the production system can be used to attack the production system in the way

- that a denial of service (availability) is achieved.
- that backdoors are established which could harm the confidentiality and integrity of the data on the production system.

© SANS Institute 2005 Author retains full rights.

Hazard 3: Infection with malicious code
A laptop with malicious code on can infect the production system when connected to it in the way
- that a denial of service (availability) is achieved.
- that backdoors are established which could harm the confidentiality and integrity of the data on the production system.

Severity, Frequency, and Risk

The next step in our safety assessment is to determine for each hazard the severity and frequency. Due to these two values the risk is directly determined according to the matrix shown in Figure 1. The results for the risks of each hazard are shown in Table 1. It should be kept in mind that the values are estimations and therefore certainly subjective. Depending on the experience of safety analysts the values will differ. When performing a safety assessment it is therefore a good practice to invite several specialists who know the systems to get averaged values for the severity and frequency.

Table 1: Results of the safety assessment before applying a policy.

Hazard No.	Hazard short description	Severity	Frequency	**Risk**	Comment
1	Remote attack	High	Medium	High	
2	Direct attack	High	Low	Serious	
3	Infection with malicious code	High	High	High	

When looking at Table 1 it was found that the deployment of laptops in a production system environment will bring one serious and two high risks to the production system!

There are now four main possibilities to handle these serious and high risks:
A) transfer,
B) accept,
C) reduce, or
D) avoid the risks.

Before serious and high risks will be transferred or accepted the security professional should normally try to find measures (within the companies budget) to reduce or to avoid the risk. To reduce the risk these measures have to reduce the severity and/or the frequency of the hazard. The measures can be for instance organisational as well as functional.

Policy Statements Step I

In this paragraph some measures are presented which are supposed to reduce or avoid the risk in our case. The measures have the character of written policy statements. This was done to be able to use and fix the measurements later in a policy about the deployment of laptops in production system environments.

© SANS Institute 2005 Author retains full rights.

The presented policy statements are relatively restrictive. They can be tailored for other environments and situations, like for instance the deployment for laptops in office communication networks which could probably result in less restrictive policy statements.
The following policy statements are focused on the laptop itself.

1. Laptops are in general not allowed to connect to the production system unless compelling reasons makes it necessary.
2. The compelling reasons are laid down in the maintenance description of the production system.
3. Only laptops with documented special authorization are allowed to connect to the production system directly.
4. A remote access of a laptop with special authorization by telephone line is not allowed.
5. The authorization of a laptop to be connected to the production system is given by the person responsible for the laptop and the manager responsible for the production system. The basis for the authorization is compliance of the system requirements within this policy. Such a laptop will be called "authorized laptop".
6. The manager responsible for the production system names a person responsible for each authorized laptop which will be documented in an authorization document.
7. The person responsible for the authorized laptop has the responsibility to ensure that this policy is enforced for his authorized laptop. He must conduct audits on a regularly basis (at least once a year) to show the compliance with the policy and document the results of these audits.
8. In a production environment where several persons must have access to the same authorized laptop (in the following called "authorized users") the person responsible for the authorized laptop will document the handing over in a special list.
9. The person responsible for the authorized laptop must give an introduction to the authorized laptop and this policy to every authorized user.
10. The authorized users of an authorized laptop are listed in the authorization document by the person responsible for the authorized laptop.
11. Authorized laptops are not allowed to connect to other systems or networks as the ones described in the maintenance documents.
12. The authorized laptop has to be stored in a safe place to ensure the integrity and confidentiality of its data.
13. The person responsible for the authorized laptop has to assure that the authorized laptop will be configured in the following way:
    - 13.1. A strong password protection has to be applied to
        - 13.1.1. the BIOS as well as
        - 13.1.2. the operating system.
    - 13.2. A login procedure has to be enforced before the access is granted.

© SANS Institute 2005 Author retains full rights.

13.3. A screen-saver with password protection has to be activated by when leaving the running authorized Laptop.

13.4. An antivirus software must be installed, maintained and updated in regularly intervals. The updates have to be documented.

13.5. A personal firewall software must be installed, maintained and updated in regularly intervals. The updates have to be documented.

13.6. All ports and services which are not necessary for the task according to the maintenance description must be deactivated and when possible uninstalled.

13.7. The BIOS must be configured in a way that the boot sequence of the hard disk will be applied unless policy requirement 19 will be applied.

14. The person responsible for the authorized laptop must name a system administrator (mostly identical) which defines, enforces, administer, and documents access rights.

15. The person responsible for the authorized laptop has to guarantee that

15.1. system backups and copies of the data as well as the software of the authorized laptop are performed and documented on a regularly basis and

15.2. backups and copies are stored in a safe place.

16. The person responsible for the authorized laptop has to assure that the actual security patches and service packs are installed to close known vulnerabilities.

17. When transferring data to the authorized laptop using storage medias (diskette, CD, DVD, memory sticks, etc.) the data as well as the storage medias must be scanned for viruses.

18. When software updates, patches and service packs are only be achievable by internet the download of them must be performed by another computer. This computer must comply at minimum to the same system requirements stated in this policy and which is preferably placed behind a firewall.

19. The person responsible for the authorized laptop should check whether the utilization of a LINUX Knoppix-Boot-CD is possible. [12]

20. Laptops are not allowed to leave the production system building unless compelling reasons makes it necessary. When it has to leave the production system building a data encryption has to be applied to the hard disk unless compelling reasons are making this impossible.

Results Step I

After writing down the policy statements concerning the laptop it has to be verified whether the measures for the laptop are really able to reduce the identified risks. For that the severity, frequency, and the resulting risk are determined again for each hazard. The results are shown in Table 2.

© SANS Institute 2005 Author retains full rights.

Table 2: Results of the safety assessment after applying the laptop policy statements.

Hazard No.	Hazard short description	Severity	Frequency	**Risk**	Comment
1	Remote attack	High	Medium	High	
2	Direct attack	High	Low	Serious	
3	Infection with malicious code	High	Low	Serious	

As can be seen, the policy for the laptop is able to reduce the frequency for hazards 3. For hazard 2 the frequency was already assumed to be low before applying the policy.
For hazard 1 the policy statements for the laptop have no real effect. Only the statements 1, 2, 3, and specially 4 could possibly be able to affect the frequency of hazard 1. But in this case it was assumed that the effect would not be sufficient enough to reduce the frequency by at least one category.

Although a good sounding and relatively restrictive policy for the laptop with 20 statements was been written, the risk for hazard 1 is still “high” and is for hazard 2 and 3 still “serious”. In summary it has to be stated that the impact of the policy statements concerning the laptop to reduce the risks are rather limited.

This limitation results from the assumed importance of the production system for the company. The severity of a hazard caused by the deployment of laptops is hard to reduce just by looking at the laptop-side. Even when the policy statements 13.6 and 16 dealing with the deactivation of ports and the installation of security patches could be able to reduce the severity of the hazards it is not assumed that they will reduce the severity from high to at least medium risk.

Policy Statements Step II

To reduce the severity of hazards the focus will be laid now on the production system itself in terms of a defense in-depth strategy. In the policy for the production system the following measures in form of statements could be stated (beyond certainly a lot of others):

21. The production system is not allowed to have any interface to establish a telephone connection.
22. All ports and services which are not necessary for the tasks of the production system must be deactivated and when possible uninstalled.
23. The person responsible for the authorized system has to guarantee that
    - 23.1. system backups and copies of the data as well as the software of the production system are performed and documented on a regularly basis and
    - 23.2. backups and copies are stored at a safe place.

© SANS Institute 2005 Author retains full rights.

24. The person responsible for the production system has to assure that the actual security patches and service packs are installed to close known vulnerabilities.
25. A standby fallback system for the production system based on different hardware and different software has to be installed and maintained.

Results Step II

The impact of the additional policy statements for the production system itself on the severity, frequency, and the resulting risk for each hazard is shown in Table 3.

Table 3: Results of the safety assessment after applying the laptop and production system policy statements

Hazard No.	Hazard short description	Severity	Frequency	**Risk**	Comment
1	Remote attack	-	-	-	Not applicable
2	Direct attack	Low	Low	Low	
3	Infection with malicious code	Low	Low	Low	

It can be seen that due to statement 21 regarding the disconnection of the production system from telephone networks the hazard 1 and therefore the related risk does not exist anymore. When the production system has no interface to telephone networks a remote attack can simply not carried out. Furthermore, especially the demand for a fallback system (statement 25) can be assumed to reduce the severity for the remaining hazards 2 and 3 to the category “low”. This leads finally to “low” risk categories for the both remaining hazards.

Due to the application of appropriate measures in form of policy statements for the laptop as well as for the production system the risk for all reflected hazards regarding the deployment of laptops in production system environments are low and could be accepted in this way.

At the end of this paragraph it should be noted that the task of a safety professional is to conduct a safety assessment, propose - if necessary - appropriate measures to reduce risks and to show the effects of this measures on the risk category. For our example this was done in the last paragraphs. It is now up to the management to decide whether all or only a part of the proposed policy statements should be realized. The management has to take into account the security as well as the company’s monetary possibilities. For instance, statement 21 regarding the disconnection of the production system from telephone networks could be realized normally without great costs but has a very great effect to the risk for hazard 1. It is therefore quite probable that the

© SANS Institute 2005 Author retains full rights.

management will agree to this requirement. A slightly different situation exists with statement 25. Fallback systems could be relatively expensive. Whether the management wants or is able to spend the money for fallback systems or whether they want to accept or transfer the remaining risk will certainly be decided carefully. But the final decision is up o the management.

Conclusion

An overall view of some existing safety and risk assessment methodologies was given at the beginning. The common way to perform a safety assessment was described. The application of a simple qualitative safety assessment method was shown in a case study for the deployment of laptops in production system environments. After the initial safety assessment measures in terms of policy statements were presented. It was shown how the measures can influence the risk category for an identified hazard. It was found that only a defense in-depth strategy considering the functional and organizational topics for the laptop as well as for the production system can lead to a sufficient risk reduction.

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

References

[1] ISO/IEC 17799:2000 (E). “Information technology - Code of practice for information security management.” First Edition. 1 December 2000.

[2] Department of Defense. United States of America. MIL-STD-882D. “Standard practice for system safety.” 10 February 2000. URL: http://acc.dau.mil/simplify/file_download.php/882d.pdf?URL_ID=8843&filename=10437060740882d.pdf&filetype=application%2Fpdf&filesize=119427&name=882d.pdf&location=user-S/&PHPSESSID=e2fb70b0f4e24582902a451d0a908f75 (15 September 2004).

[3] NASA. M.G. Stamatelatos. “Risk Assessment and Management, Tools and Applications.” Presentation. URL: http://smo.gsfc.nasa.gov/riskman/presentation_1.pdf (15 September 2004).

[4] NASA. NPR 8715.3. “NASA Safety Manual.” 31 March 04. URL: http://nodis3.gsfc.nasa.gov/displayAll.cfm?Internal_ID=N_PR_8715_0003_&page_name=all (15 September 2004).

[5] EUROCONTROL. Safety Assessment Methodology. Edition 2.0. 30 April 2004. URL: http://www.eurocontrol.int/safety/downloads/sam/Level1/SAM%20V2-0%20intro.doc (15 September 2004).

[6] EUROCONTROL. Safety Assessment Methodology, Edition 2.0. 30 April 2004. Guidance Material E. “Risk Classification Scheme.” URL: http://www.eurocontrol.int/safety/downloads/sam/Level2/FHA%20V2.0/FHA%20V2-0%20Chapter%203%20Guidance%20E.doc (15 September 2004).

[7] EUROCONTROL. Safety Assessment Methodology. Edition 2.0. 30 April 2004. Guidance Material D. “Severity Classification Scheme.” URL: http://www.eurocontrol.int/safety/downloads/sam/Level2/FHA%20V2.0/FHA%20V2-0%20Chapter%203%20Guidance%20D.doc (15 September 2004).

© SANS Institute 2005 Author retains full rights.

[8] EUROCONTROL Safety Assessment Methodology and Guidance Material. Edition 2.0. 30 April 2004.
URL: http://www.eurocontrol.int/safety/GuidanceMaterials_SafetyAssessmentMethodology.htm (15 September 2004).

[9] Federal Aviation Administration. Office of System Safety. Overview.
URL: http://www.asy.faa.gov/Risk/ (15 September 2004).

[10] Federal Aviation Administration. “System Safety Process Steps.“ Revision 1. February 2003.
URL: http://www.asy.faa.gov/Risk/SSProcess/SSProcess.htm (15 September 2004).

[11] Federal Aviation Administration. “System Safety Handbook.” 30 December 2000.
URL: http://www.asy.faa.gov/Risk/SSHandbook/cover.htm (15 September 2004).

[12] Klaus Knopper. KNOPPIX.
URL: http://www.knopper.net/knoppix/index-en.html (15 September 2004).

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.