Information Risk Assessment - How to get it right

Daniel Fischer[1]
European Space Agency, Darmstadt, Germany

Information Security is a topic of growing concern within the space community. In particular ground control systems and space-link communications are required to ensure a minimum level of security and robustness. Security requirements are usually established using information risk assessment which evaluates the target systems' vulnerabilities and establishes the identification of potential threats. From this point, the risk assessment evaluates the likelihood of a threat against the severity of identified vulnerabilities and determines a quantifiable risk for each of these combinations. Many risk assessment methodologies such as ISO27005, NIST SP 800-30, or EBIOS exist, but they all face similar problems in practice. The risk assessment process looks easy on paper – but experience within ESA has shown that it can turn into a complex nightmare with unusable results if it is not done right especially when applied to complex systems. In our paper, we address the main pitfalls of risk assessment and how to avoid them. Our contribution is the result of the analysis of a number of ESA risk assessment exercises lessons learned. Some of these risk assessments were very successful while others were not. We elaborate on the following central buzzwords of successful risk assessment: Know your system, Know what is important for your system, Keep it simple, Don't believe you are done after the first round.

I. Introduction

SPACE mission and program systems and infrastructures are very often big, complex, distributed and they are in many cases unique or at least very different to each other. Such infrastructures are composed of hardware systems (e.g. ground stations, spacecraft hardware), software systems (e.g. the mission control software or the spacecraft onboard software), and communication channels and often from systems-of-systems. Each infrastructure has to meet the requirements set forward by the mission or program stakeholders. While there are often components that can be re-used or that are multi-purpose, the final composition of these components into an overall system or even system-of-systems is quite unique.

With the more and more ubiquitous and ever-increasing amount of security threats that apply even to civilian missions today, it is important that space mission systems are appropriately protected against these threats. In order to design and develop and appropriate security infrastructure that is able to reduce the risks resulting from these threats below an acceptable level, a proper information risk assessment exercise has to be executed and continuously repeated during the whole development lifetime of the system – from drawing board to operations. The proper execution of an information risk assessment for a complex system or system-of-systems poses a significant challenge. This paper addresses some of the pitfalls that can be encountered in this process and gives hints how to avoid them.

A. Contribution

In this paper, we look at the central process of information risk assessment and we highlight the pitfalls that one has to consider and take into account in order to reach a satisfactory conclusion and useful results of the risk assessment exercise. A number of past and also still ongoing risk assessment exercises and their lessons-learned form the foundation for this assessment. Our recommendations should be valid for all major information risk assessment methodologies available on the market. In this paper, we address the following issues:

1) Know your system before starting an information risk assessment
2) Be sure you know what pieces of information are critical in your system or system-of-systems
3) Keep it simple – abstract where possible and only consider relevant information
4) Don't believer that you are done after the first round – information risk assessment is an iterative process

[1] Data Systems Manager, Ground Systems Engineering Department, Daniel.Fischer@esa.int

5) Ensure that information risk assessment is independent

We will elaborate on the above points and hope to help engineers to avoid these major pitfalls.

B. Organization of the Paper

This paper is organized as follows. In Section II we provide a short introduction to information risk assessment and also review the most popular available information risk assessment methodologies. Section III forms the heart of this paper and looks at the four major pitfalls stipulated above. Finally, Section IV provides a conclusion.

II. Information Risk Assessment

This Section introduces the concept of information risk assessment, describes the various steps, surveys the major currently available methodologies, and addresses the specific challenge of information risk assessment for systems that have space components.

A. What is Information Risk Assessment?

Information risk assessment is a term without an unambiguous definition. Different sources will provide different definitions. In this paper, we consider information risk assessment as per definition made in ISO/IEC 17799:2005[1] and NIST 800-30[3] which is also the context in which it is used within the ESA ground segment engineering department.

The main objective of information risk assessment is the identification, quantification, and prioritization of risks for the system or system-of-systems to be analyzed. Two main steps make up the process of information risk assessment – risk analysis and risk evaluation. Risk Analysis is the process to identify the risks that apply to the system or system-of-systems in question. Risk Evaluation builds upon risk analysis, quantifies the identified risks and identifies their criticality to the system or system-of-systems that is being investigated. Figure 1 shows the general steps associated with an information risk assessment exercise as well as the required input for each step of the process.

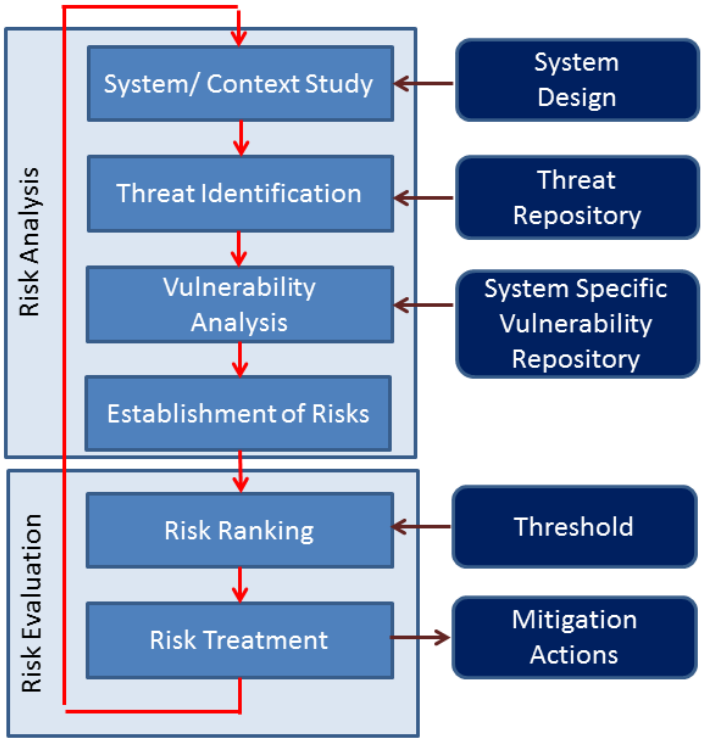

Figure 1. Information Risk Assessment Process. *While the process of the information risk assessment exercise is slightly different in each standard, the principals steps are identical.*

The risk analysis phase starts with the identification of threats that are applicable to the system or system-of-systems under analysis. Threat lists are often universal and security institutes and bodies publish generic threat lists that can be taken as input to the threat identification process. An example is the list of elementary threats[2] that is published by the German Federal Office for Information Security. NIST[3] also provides a high-level list of threats. However, some tailoring is required for each risk assessment exercise. The threat analysis is followed by the vulnerability analysis. Other than for the threat analysis, a generic list of vulnerabilities usually does not exist since they are very specific to the system or system-of-systems under investigation. The sources for the provision of vulnerabilities are multiple: past experience, lists of vulnerabilities that are applicable to specific systems (e.g. OWASP[8] in the case of a SOA-based software system or the NIST I-CAT database[9], results of security analysis etc. The vulnerability analysis is usually followed by the likelihood determination and the impact analysis. The result of the process is a list of risks that are specific to the system or system-of-systems that is being assessed.

The list of risks which is produced by the risk analysis is used as input for the risk evaluation. For each risk that applies to the system or system-of-systems under investigation, it will have to be evaluated whether the risk will be

mitigated (i.e. appropriate security controls will be put in place to reduce the risk), accepted (i.e. the risk is acknowledged and accepted without countermeasures) or transferred. In order to be able to make this decision, a so called risk threshold will have to be established. Risks that exceed this threshold are deemed to be unacceptable and need to be mitigated. Please note that mitigated risks do not disappear, they are just reduced to a value that lies below the threshold line by putting appropriate security controls in place.

It is obvious that the process of risk assessment (i.e. risk analysis and risk evaluation) will have to be repeated for a system or system-of-systems in regular time intervals. The first iteration however is usually the most resource-intensive while the following iterative assessments can build on the results of the previous one.

B. Security Requirements

An initial step for the definition of a security architecture for each system or system-of-systems is the specification of security requirements. A number of security requirements are implicit and will be inherited from the corporate security guidelines and procedures as well as from mission-specific security objectives of the system or system-of-systems to be defined.

A good example for the first category are security requirements inherited from corporate or Agency-wide security regulations such as the protection of classified information. Security requirements on how to deal with and handle information with certain classification levels are dictated to the project by the security regulations.

The second category are security requirements that are needed to support one or more of the business / mission-specific objectives of the project. For example, a system could involve a control center and a spacecraft with explicit user requirements for authentication of telecommands that are transferred from the control center to the spacecraft. This would imply security requirements for the authentication.

These two categories of security requirements are obvious and usually a fixed contribution and can be considered the user requirements for the system or system-of-systems to be defined. The third category comes into play usually only as part of the specification of the system requirements. These are security requirements that are an outcome of an initial round of the information risk assessment. They basically address all the security needs of the system that are not directly specified by the user security requirements. The number and strictness of these security requirements are directly dependent on the choices made during the initial information risk assessment.

It should be noted, that as mentioned above, information risk assessment is an iterative process. Thus, security requirements specified as result of the initial information risk assessment may be revised and/or refined at later stages in the early design phase by subsequent follow-up iterations.

C. Security Controls Selection

In Section II.A it is mentioned that during the risk evaluation so called security controls will be put in place to mitigate risks and reduce their risk values to below the threshold line. Security controls can be either abstract in an early project phase (e.g. during a system-of-systems architectural design phase) or very concrete and system specific for example in the case of a software development project. For both cases usually there are lists and general recommendations available from different sources that can be tailored and applied to the information risk assessment process.

D. Risk Assessment Methodologies

Different risk assessment methodologies from various groups and organizations exist. Some of them are in particular tailored to a certain classes of systems (e.g. a software systems) others are really generic and can be applied to any kind of system or system-of-systems. It has to be noted however that those methodologies are still very similar and that all contributions of this paper apply to all these methodologies. We provide a brief survey of the most popular risk assessment methodologies.

1. ISO/IEC 27005

As part of the 27000 series, ISO has specified its own risk assessment methodology, the ISO/IEC 27005[4]. The ISO 27005 is part of the ISO 27000 series of standards which deal with security techniques for information technology. Since it is an international standard, it is probably the most popular risk assessment methodology from the list presented in this paper. It fits in seamlessly, in terms of terminology and concepts, with the ISO 27001, which is the most famous of the standards in this family. It is widely compatible with the EBIOS and BSI methodologies and provides not only a risk assessment methodology, but also a high-level list of vulnerabilities and threats. ISO 27005 is very much focused on information technology systems.

2. NIST 800-30

The NIST 800-30: Risk Management Guide for Information Technology Systems[3] by the US National Institute of Standards and Technology is, as the ISO 27005, directly focused on IT systems and in particular software. It

contains many references and guidelines on how to integrate the information risk assessment into the software development lifecycle. It is in many ways more abstract and less formal than the ISO 27005 an, as it name says, provides more guidelines for risk assessment that an actual process. Nevertheless all the steps for risk analysis and evaluation are well documented.

3. EBIOS

EBIOS – or Expression des Besoins et Identification des Objectifs de Sécurité[5] – is a risk assessment methodology that has been developed by the French National Security Agency (ANSSI/ACE/BAC). It is the most detailed of the risk assessment methodologies listed in this paper and it is also not only focused on information technology, but on any kind of system or in particular system-of-systems in general. This is the reason why it is very popular for use in complex systems that are not limited to IT components and it is used very much also outside France. The current version, EBIOS 2010, is compatible with the ISO 27005, however it is only available in French so far.

4. BSI

The BSI Standard 100-3 – Risk Analysis based on IT Grundschutz[6] – is very closely related and actually dependent on the BSI Standard 100-2 – IT Grundschutz Methodology[7]. It is published by the German Federal Office for Information Security and is, as ISO and NIST, very closely related to IT technology. In fact from the methodologies listed here, it is probably the one that is closest to IT. It does not provide a real risk assessment methodology as such but is rather focused providing a risk assessment frame to the methodologies specified in BSI Standard 100-2.

5. Summary

The list of risk assessment methodologies above is not exhaustive. Many more methodologies exist, however, were not used or consulted by the authors of this paper. It can be said, that in general the ISO risk assessment method has been established as the de-facto standard and other methodologies tend to become aligned with the ISO, while often being more detailed or having a different focus.

E. Space Business Risk Assessment Challenges

Most of the recommendations in this paper can be considered generic and would apply to any (complex) system or system-of-systems. Yet, space-related systems usually pose additional challenges for risk assessment experts. The reason in many cases lies with the specific environment. Many threats, vulnerabilities, and consequently risks are present in a system involving space components that cannot be found in terrestrial systems (e.g. vulnerabilities related to the communication between a ground station and a spacecraft). Thus it is not so easy to rely on existing threat and vulnerability catalogues when doing a space system risk assessment. Thus it is advisable to build a proprietary set of catalogues and keep them up to date. This may imply some overhead on the first risk assessment runs but makes it easier for later iterations. Furthermore, it is crucial that this is done at corporate level and not confined within one mission or project. Management support is thus paramount in this respect. The above is especially true of systems-of-systems which are even more complex than single systems.

III. Information Risk Assessment Pitfalls and how to avoid them

In this Section, we provide guidelines and recommendations to handle or avoid pitfalls which typically occur when executing and information risk assessment. We focus particularly on complex systems or system-of-system infrastructures which pose specific challenges for information risk assessment.

A. Things that can go wrong

When executing an information risk assessment for your system or system-of-systems under development, a number of things can go wrong and some of them have the potential to turn the information risk assessment into a nightmare of hundreds of numbers that are of no practical use for the system development. If done right, risk assessment will provide you with a small number of well-identified top risks for which security controls must be put in place to mitigate them (specified as security requirements). Below is a list of the most critical problems that can arise during risk assessment and for which solutions are outlines in the following Sections.

- The information risk assessment produces only highly-generic risks that are not tailored to the particularities of the system.
- The information risk assessment produces risks that in reality are not as critical as the risk assessment describes them- a consequence of wrong criticality assignment for primary assets

- The information risk assessment produces a huge matrix of complex risk values instead of a clear list of a risks to be mitigated. This is a danger in particular for complex systems as they are common in the space business – for example a mission control infrastructure.
- The results of the information risk assessment are not in line with the reality of the system architecture. Instead they are more representing the system architecture as it was envisaged in early design phase/ requirements engineering.
- The risk assessment results are incomplete and a number of potentially critical risks are not present in the mitigation list.

B. Know your system before you start the risk assessment

Information risk assessment is an activity that starts in parallel with the development of the system or system-of-systems. This means information risk assessment needs to start while not much information on the system to be assessed is available since the design of this system is not yet in an advanced state. However, all risk assessment methodologies require as initial step the establishment of understanding concerning the system to be analyzed. ISO 27005 calls this "Context Establishment" while EBIOS calls it "Context Study". This initial first step is crucial for the information risk assessment since it establishes the boundaries of the system and also indicates a number of system-specific properties that may be of special importance to the risk assessment.

The inherent danger with not feeding already high-level system specific information into the context establishment is that the first iteration of the information risk assessment will be very wide in scope and the results will not be useful. This means for example that the lists of threats, vulnerabilities, and ultimately risks would be so generic that they would be applicable to a large number of different systems. In this case, the information risk assessment would have added no value at all. Furthermore, if the scope is too generic, follow-up iterations of the information risk assessment suffer the problem that they will have to take the outputs of the previous iterations, which were too generic, into account. This can very easily lead to a huge increase in complexity.

It is therefore critical that at least the high-level characteristics and particularities of the system or system-of-systems to be analyzed is passed as input into the context establishment of the information risk assessment. In particular, usually at this step, customer requirements or a similar definition of the user needs exist, which can be fed into the context establishment. It will give the risk assessment engineer a good idea of the system that will be developed and he can already limit the scope of the first iteration of the information risk assessment.

It is important that the context study is repeated for each iteration of the information risk assessment although it may seem as a very good candidate to skip. The fact however is that the more the system design processes the more detailed information can be passed to the information risk assessment during the context study, making the results more precise.

C. Be sure you know what is important for your system

This concern is in very close relationship to what was addressed in Section III.B above, however it is not only relevant for the first iteration of the information risk assessment but stays vital during the whole development phase. As part of the context establishment, the primary assets identified will be assigned a so called CIA level. CIA refers to the three major security criteria – Confidentiality, Integrity, and Availability. The assignment of the CIA levels to primary assets will have a critical impact on the risk levels that the risk analysis will produce for these asset.

This sensitive task is very often left for the asset or system owner alone to perform. Owners and stakeholders however are often not very familiar with security terms and cannot properly distinguish between the three aspects of CIA or evaluate when to assign which level. It is important that their input is not just accepted, but critically evaluated with their involvement. Thus, the owner should be involved in the CIA assignment process, however it is absolutely essential that he is assisted by an information risk assessment expert. This expert can interact with the owner, explain the CIA scales, and make clear what the consequences of too high or too low values for the CIA levels will be.

It is the experience of the authors that, if such involvement is not provided, the CIA level assignment will be too high in many cases. In the later phases of the information risk assessment, this would lead to a large number of high risks that require expensive mitigation issues to be put in place. It is very often only at this point (mitigation) that the errors being made at the CIA assignment are uncovered since only then the budget available for the risk mitigation measures comes into play.

D. Keep it simple – Only consider the relevant

The complexity of an information risk assessment exercise can very quickly develop into a problem and may cause substantial overhead in effort and other resources that are consumed in the process. Furthermore, as a consequence, the later steps of the risk assessment can turn into a complex mathematical exercise that produces a huge amount of numbers and value for an equally huge amount of risks identified. Keeping in mind the goal to reduce the risk level for risks affecting the system or system-of-systems, this may be very hard to achieve since such overly complex results are not easy to read by engineers. It is crucial that the risk assessment team keeps it simple – others need to understand and interpret the results.

There are two major things to remember when executing a risk assessment on a complex system or system-of-systems: Be careful with generic risks and divide and conquer. Taking these two things into account will significantly reduce the probability that the output of the information risk assessment will be a spread sheet nightmare.

The first point is very closely related to what is said in Section III.C. The less specific information you have on your system's primary assets and their security needs, the less precise or system-specific your information risk assessment will be. This means that a potentially large number of generic aspects are considered as part of the information risk assessment that do not really represent the systems primary assets. These generic risks will at the be combined with the concrete risks based on very concrete system information thus leading to a less precise result of the risk assessment. Since the risk evaluation will need to find a decision concerning which risks are critical and which mitigation issues need to be funded, this is a non-trivial problem. Generic information should thus be avoided or at least cross-checked before being fed into the information risk assessment during the context study step.

The second point is more critical for complex systems or systems-of-systems. The more diverse and complex the system to be analysed is, the more threats, vulnerabilities, and eventually risks will have to be considered during the information risk assessment. In many cases, a divide-and-conquer approach is more beneficial. Concretely this means that the complete system shall be broken down into subsystems with well identified interfaces between each other. Figure 2 visualizes such a breakdown for a mission control infrastructure. In this way, one complex risk assessment exercise can be broken down into several smaller and more simple ones. This smaller information risk assessments would be applied only to specific subsystems, taking into account the well-defined interfaces to other subsystems. Once all risks for the subsystems have been identified, a global risk assessment exercise that takes into account the results from the individual risk assessments can be conducted to combine the results.

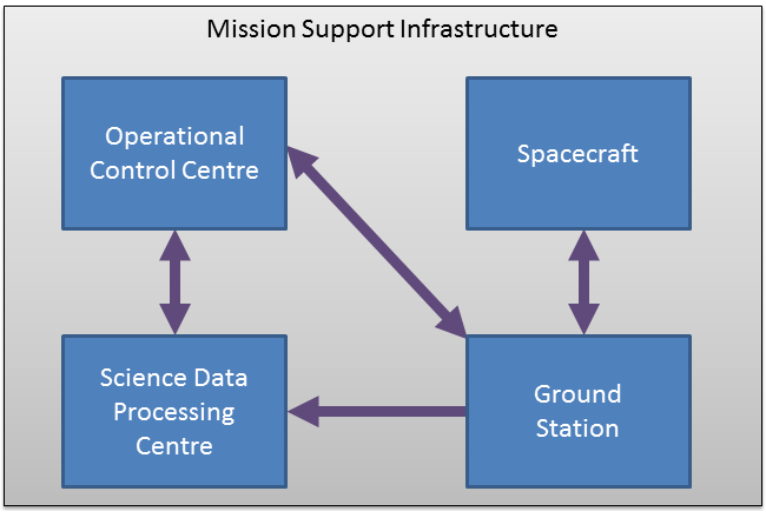

Figure 2. Risk Assessment Divide and Conquer Example. *In this case individual risk assessment exercises would be executed for the four subcomponents before their results are being fed back into a global risk assessment exercise for the mission support infrastructure. It is important that interfaces such as the space-link data flow are being considered already for the individual risk assessment exercises.*

E. Don't believe you are done after the first round

It is often believed that information risk assessment is a one off process during the development of a new system or system-of-systems. Once the risk assessment has produced the security requirements and the security controls to mitigate the identified risks, no further risk assessment activities are considered. In most cases this is a decision related to the saving of resources and effort.

However, it is paramount to understand that information risk assessment is an iterative process. It is one of the first steps in the system development lifecycle but also one of the last as well. Identified risks have to be re-visited constantly during the system development. Very often new risks are introduced (e.g. because a new design technology is selected) and have an impact on the outcome of the previous risk assessment iteration. However, it can be noted that from an effort point of view, the first information risk assessment round is the most costly. But he

following iterations can usually build on and re-use parts of the outcome of previous iterations, resulting in an acceptable overhead. This paradigm of constant re-iteration is getting even more important with the advent of new development methodologies such as agile development.

F. Ensure that information risk assessment is independent

In many cases, system developers tend to execute the information risk assessment themselves as part of the development process. While this saves valuable resources, the results of the information risk assessment will always be biased. For example, a number of threats may not be considered at all just because the system was not designed with these threats in mind. As a consequence, a critical review of the risks applicable to the system or system-of-systems under development cannot be achieved and a number of risks may remain unidentified. It is therefore of paramount importance that the information risk assessment is executed by an independent team of risk assessment experts. This could be an internal team, for example a security office which is specialized for this, or an independent entity. Many security companies are specialized in the execution of information risk assessments for their customers.

The independent risk assessment team should interact constantly with the security experts involved in the development in order to ensure that security controls identified during the risk assessment are properly implemented. Furthermore, interaction with the development team is necessary in the first phase of a risk assessment iteration, the context study.

IV. Conclusion

Information risk assessment is one of the central processes required when developing a new system or system-of-systems. Ideally, its results help to identify the security controls that need to be implemented as part of the system in order to reduce identified risks (mitigation). But information risk assessment has often added more overhead than actual added value, especially when applied to complex, distributed systems or systems-of-systems that are very common in the space business. It is therefore crucial to know these "pitfalls" of information risk assessment and how to avoid them. If properly done, information risk assessment can deliver clear results and really help to make a newly developed system secure without creating a huge amount of overhead. In this paper, we have collected a few hints and recommendations that from our experience help to achieve an optimal and helpful result for the risk assessment. Currently, we are testing these guidelines in the information risk assessment process for a very complex system-of-systems that is in its early design phase.

Appendix A
Acronym List

CIA	Confidentiality Integrity Availability
EBIOS	Expression des Besoins et Identification des Objectifs de Sécurité
ESA	European Space Agency
ISO	International Standards Organization
NIST	National Institute of Standards and Technology

Appendix B
Glossary

The definitions in this Glossary are taken (in some cases slightly modified) from NIST 800-30[3].

Availability — The security goal that generates the requirement for protection against—

- Intentional or accidental attempts to (1) perform unauthorized deletion of data or (2) otherwise cause a denial of service or data
- Unauthorized use of system resources.

Confidentiality	The security goal that generates the requirement for protection from intentional or accidental attempts to perform unauthorized data reads. Confidentiality covers data in storage, during processing, and in transit.
Integrity	The security goal that generates the requirement for protection against either intentional or accidental attempts to violate data integrity (the property that data has when it has not been altered in an unauthorized manner) or system integrity (the quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation).
Risk	The net mission impact considering (1) the probability that a particular threat-source will exercise (accidentally trigger or intentionally exploit) a particular vulnerability and (2) the resulting impact if this should occur.
Information Risk Assessment	The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact.
System-of-Systems	System of systems is a collection of task-oriented or dedicated systems that pool their resources and capabilities together to create a new, more complex system which offers more functionality and performance than simply the sum of the constituent systems.
Threat	The potential for a threat-source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.
Threat Source	Either (1) intent and method targeted at the intentional exploitation of a vulnerability or (2) a situation and method that may accidentally trigger a vulnerability.
Vulnerability	A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.

References

[1] ISO/IEC 27002, Information technology - Security techniques - Code of practice for information security management, June 2005

[2] German Federal Institute for Information Security, Threats Catalogue – Elementary Threats

[3] NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems, July 2002

[4]ISO/IEC 2005, Information Technology – Security Techniques – Information Security Risk Management, June 2008

[5]ANSSI/ACE/BAC, EBIOS – Méthode de gestion des risques – 25 January 2010

[6]BSI Standard 100-2 IT-Grundschutz Methodology, 2.0, 2008

[7]BSI Standard 100-3 Risk Analysis based on IT-Grundschutz, 2.5, 2008

lude any cataloging information that may be provided. Always query for an update if a work is about to be published.

[8] The Open Web Application Security Project (OWASP) – http://www.owasp.org

[9] National Vulnerability Database v 2.2 -http://nvd.nist.gov/