

Chapter 2 – INTRODUCTION

2.1 RATIONALE

During the 7th IST panel an exploratory team titled “Improving security awareness” was proposed. Following the 11th of September events in USA, the new focus put on anti-terrorism activities conducted the Panel Members to rename the exploratory team to “Improving common security risk analysis” during the 8th IST panel.

Today many NATO nations use national risk analysis methodologies (for example EBIOS for France, CRAMM for UK, ITSG-04 for Canada, MAGERIT for Spain). These methodologies, even if based on similar principles, use different threat and vulnerabilities classification. The increase of interoperability between national and NATO systems requires building up a common risk analysis methodology. A Canadian contribution received in September 2001 pointed up the need for a common NATO classification for threats and vulnerabilities.

To counter or mitigate the gaps in NATO capabilities against Cyber Defence, the Heads of State and Government agreed at the Prague Summit to improve Cyber Defence in NATO. The capability to continuously assess and manage the risk has been identified **as a priority 1 measure**.

This activity can be linked with the following requirements from NATO strategic commands (from the document RTO programme and NATO requirements: RTA/SPD (2004-03) PG2004):

- MF03: Intelligence support: need for a real time NATO security alert system (page 22).
- MF03: Need to develop intelligence collection and analysis tools (page 23).
- MF03: Need for advanced analytical tools for threat assessment (page 24).

And with Defence capabilities initiatives:

- Sustainability and logistics: NATO nations should enhance interoperability ... (page 88).
- Survivability of forces and infrastructure: the alliance shall review the vulnerability ... (page 107).

2.2 REFERENCES TO RISK ASSESSMENT AND RISK ANALYSIS WITHIN NATO DOCUMENTATION

C-M(2002)49: Security within the North Atlantic Treaty Organisation, enclosure F, §15: “Systems handling NATO classified information, in NATO civil and military bodies, shall be subject to risk assessment and risk management in accordance with the requirements of directives supporting this policy.”

AC/35-D/2004: Primary directive on INFOSEC: Security Risk Assessment and Risk Management, §11 to 18.

AC/35-D/2005: INFOSEC Management Directive.

2.3 ROLE OF RISK ANALYSIS

Everyone takes and manages risks all the time, balancing potential rewards against uncertain losses. Risk management remains nevertheless a very difficult process. It requires combining the “hard”

INTRODUCTION

scientist's approach, who treats risks as something that can be objectively measured, with the view of the "social" scientist who argues that risk is a fuzzy concept and the propensity to take risks is in part culturally constructed.

A *risk* is the chance of something going wrong as a result of a hazard or a threat which has an impact on operations. Risks arise out of uncertainty. A risk is measured in terms of its likelihood of happening and the consequences if it should happen. *Risk management* is balancing the cost of avoiding, reducing, transferring or accepting a risk with the benefits that can be expected from taking the risk.

Taking a risk incurs the *possibility* of suffering loss. This loss may or may not happen. When a negative event or issue is a certainty, it is considered to be a *problem*, not a risk. Problems are out of the scope of the risk management process.

The term *risk management* is used in a wide variety of disciplines, and itself also combines concepts and techniques from a range of fields like statistics, economics, operations research and decision theory.

When different organizations need to put in place a link between their information systems in order to exchange privileged information, for instance in the context of a "Global Information Grid" (GIG), it is necessary to manage the risks that such a link inevitably introduces.

Unfortunately, there are no standards for defining vulnerabilities and threat-sources, assigning and combining impact and probability ratings, or introducing the impact of controls in the field of information security related risk management. Different methodologies and tools use different definitions and approaches. It is therefore difficult to import the risks identified and assessed by a coalition member for his system in a straightforward way into another coalition member's risk management process.

Recent standards and recommendations on the management of information systems and organizing the protection of information security within an organization widely recognize the importance of information security related risk management.

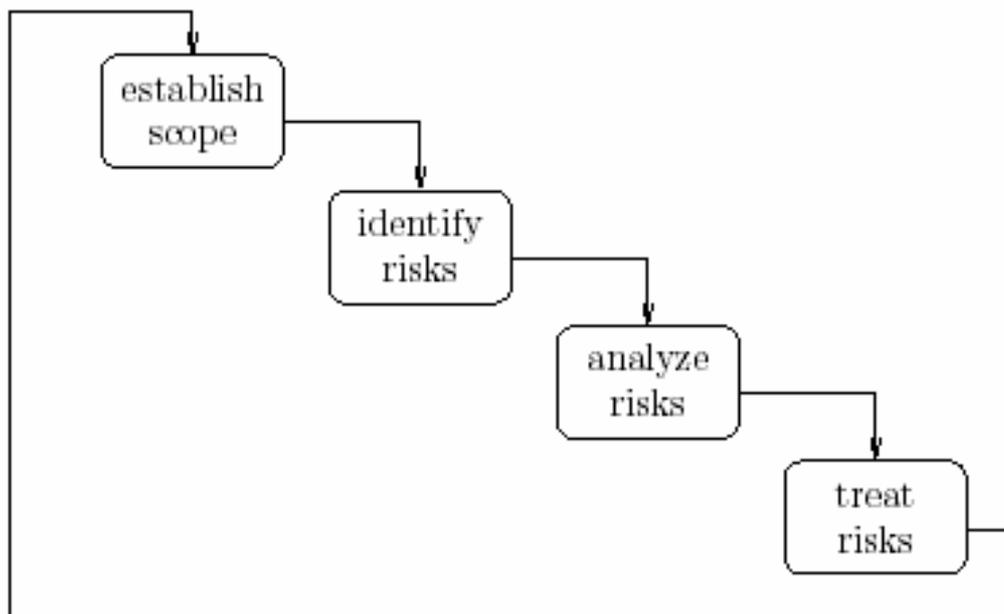


Figure 2-1: Risk Management Process.

Risk management processes typically include the following four steps:

- **Establish the Scope**

The first step in any risk management process consists in defining the scope of the risk management process, in other words the information system that is the target of the evaluation, its boundaries and environment, as well as the identity and objectives of the stakeholders.

The characterization of the system must be as complete as possible and most often includes the following elements:

- Hardware (e.g. servers, workstations, network equipment);
- Software (e.g. operating systems, system services, application software);
- Connectivity (internal and external);
- The information system's mission;
- The information that is managed by the system and its requirements regarding availability, integrity and confidentiality;
- Support staff and users; and
- Existing controls: technical controls (e.g. user identification and authentication equipment, encryption hardware and software), management controls (e.g. security policy, acceptable use policy), operational controls (e.g. backup and contingency operations, off-site storage, user account creation and deletion procedures), physical security environment (e.g. site security, data center policies), environmental security (e.g. controls for power, temperature, humidity).

- **Identify the Risks**

The second step of the risk management process consists in establishing a list of the risks to which the information system is exposed.

First, based on the system and context description available at the end of the previous step, the vulnerabilities that apply to the target of the evaluation are identified.

A *vulnerability* is any flaw or weakness in the design of a system, in its implementation or in the controls that are in place to protect it, that can result in damage when it is accidentally triggered or intentionally exploited.

A *threat-source* is either the combination of the intent and the means to intentionally exploit a vulnerability (e.g. a thief, a disgruntled employee) or a situation that may accidentally trigger a vulnerability (e.g. an earthquake, a sloppy user).

A threat is the potential for a threat-source to accidentally trigger or intentionally exploit a vulnerability. When for a given vulnerability there is no threat-source that has the technical ability or motivation to exploit it, there is no threat. Likewise, when there is no vulnerability present for which a given threat-source has the necessary skills, time and budget, this threat-source poses no threat.

Each threat is after that matched with the list of controls that were identified in the first phase, and that mitigate the likelihood of a vulnerability being exercised or reduce the impact of such an adverse event when it occurs. The resulting tuple (threat, threat-source, list of relevant controls) defines the risk that will be assessed and treated in the subsequent steps.

INTRODUCTION

- **Analyze the Risks**

In this step, the risks that were identified, are to be analyzed in more detail, so that in the step hereafter the minor, acceptable risks can be separated from the major risks which must absolutely be eliminated or reduced.

This involves deriving for each risk an overall likelihood rating that indicates the probability that the vulnerability may be exercised by the corresponding threat-source. The second element in risk assessment is trying to rate the adverse impact of the vulnerability when it were to be exercised. This rating will be based on an evaluation of the loss or degradation of integrity, availability, and confidentiality of the information that is threatened by the vulnerability.

When determining the probability and impact of a threat, the existing controls that reduce the likelihood or impact and their adequacy have to be taken into account.

The combination of probability and impact will finally be translated into a single level of risk to the information system, for instance using a risk-level matrix.

- **Treat the Risks**

Risks can be handled in a number of ways:

- *Risk Avoidance*: means simply not performing the activity that carries the risk.

Unfortunately this also typically means losing out on the potential gain that performing the activity might have produced.

- *Risk Reduction*: involves approaches that reduce the probability of the vulnerability being triggered or reduce the impact when the vulnerability is triggered.

Reducing a risk most often involves putting in place controls.

- *Risk Transfer*: means passing the risk on to another party that is willing to accept the risk, typically by contract or by hedging.

Insurance is an example of risk transfer using contracts.

- *Risk Retention*: means accepting the loss when it occurs.

Risk retention is a viable strategy for small-impact risks where the cost of insuring against the risk would be greater over time than the total losses sustained.

Also, all risks that are not avoided nor transferred, and that one does not can or wish to reduce any further, automatically fall under this category. This includes risks that are so large or catastrophic that they either cannot be insured against or the premiums would be infeasible.

The combination of methods used to handle each of the risks that were identified, analyzed and treated, leads to a risk management plan, that must then be implemented.

Risk management can be performed once for a given system, for instance before it comes in operation, and then periodically updated during the lifetime of the system. The back coupling, shown in Figure 2-1 above, is in this case not permanent but rather periodically triggered. Risks management can however also be conceived as a continuous process and influence decision-making at all instances through the life of the system.

2.4 GLOSSARY

Term	Definition	Source
Acceptable Risk	A judicious and carefully considered assessment by the appropriate Designated Approving Authority (DAA) that an information technology (IT) activity [system], or network meets the minimum requirements of applicable security directives. The assessment should take into account the value of IT assets; threats and vulnerabilities; countermeasures and their efficiency in compensating for vulnerabilities; and operational requirements.	CSE ITSG-04
Accountability	Property that allows the ability to identify, verify, and trace system entities as well as changes in their status. Accountability is considered to include authenticity and non-repudiation.	NIST SP800-37
Accountability, security goal	The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This support non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.	NIST SP800-30
Asset	Information or resources to be protected by the countermeasures of a Target Of Evaluation (TOE). Assets types include: information, hardware, communications equipment, firmware, documents/publications, environmental equipment, people/staff, infrastructure, goodwill, money, income, organizational integrity, customer confidence, services and organizational image.	Common Criteria CSE ITSG-04
Asset, Value	A measure of asset worth in terms of replacement cost, confidentiality, integrity, availability [or other elements]. Values vary from asset to asset. They are used for many purposes such as representing levels of importance to the “business” or operations/operational mission of an organization.	CSE ITSG-04
Assurance [security objectives]	Ground for confidence that an entity meets its security objectives.	Common Criteria
Attack	The act of aggressively trying to bypass security controls on an IT system or network. The fact that the attack is made does not mean it will succeed. The success depends on the vulnerability of the system, network or activity and the effectiveness of the safeguards in place.	CSE ITSG-04
Attack potential	The perceived potential for success of an attack, should an attack be launched, expressed in terms of an attacker’s expertise, resources and motivation. [Similar to threat level for threat scenarios]	Common Criteria

INTRODUCTION

Term	Definition	Source
Availability	The security goal that generates the requirement for protection against: <ul style="list-style-type: none"> • Intentional or accidental attempts to: <ol style="list-style-type: none"> 1) Perform unauthorized deletion of data; or 2) Otherwise cause a denial of service or data. • Unauthorized use of system resources. 	NIST SP800-30
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.	NIST SP800-30
Countermeasures	Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards.	NIST SP800-53
Criticality/sensitivity	A measure of the importance and nature of the information processed, stored, and transmitted by the IT system to the organization's mission and day-to-day operations.	NIST SP800-37
Denial of Service	The prevention of authorized access to resources or the delaying of time-critical operations.	NIST SP800-30
Impact	A measure of the degree of damage or other change caused by a threat event.	CSE ITSG-04
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).	NIST SP800-30
IT-Related Risk	The net mission impact considering: <ol style="list-style-type: none"> 1) The probability that a particular threat-source will exercise (accidentally trigger or intentionally exploit) a particular information system vulnerability. 2) The resulting impact if this should occur. IT-related risks arise from legal liability or mission loss due to: <ol style="list-style-type: none"> a) Unauthorized (malicious or accidental) disclosure, modification, or destruction of information; b) Unintentional errors and omissions; c) IT disruptions due to natural or man-made disasters; or d) Failure to exercise due care and diligence in the implementation and operation of the IT system. 	NIST SP800-30
Residual Risk	The risk that remains after risk treatment.	ISO 17799

Term	Definition	Source
Risk Acceptance	An action taken by the responsible manager to declare and be held accountable for acceptance of the remaining or residual risks attributed to an IT system after the performance of a threat and risk assessment. Generally, the acceptance of the residual risk is made because any further addition of safeguards does not justify the effort in terms of cost or functionality.	CSE ITSG-04
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. Part of Risk Management and synonymous with Risk Analysis.	NIST SP800-30
Risk Management	The total process of identifying, controlling, and mitigating information system–related risks. It includes risk assessment, cost-benefit analysis, and the selection, implementation, test, and security evaluation of safeguards. This overall system security review considers both effectiveness and efficiency, including impact on the mission and constraints due to policy, regulations, and laws.	NIST SP800-30
SISRS	System Interconnection Security Requirement Statement	
Threat	The potential for a threat-source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.	NIST SP800-30
Threat-source	Either: <ul style="list-style-type: none"> 1) Intent and method targeted at the intentional exploitation of a vulnerability; or 2) A situation and method that may accidentally trigger a vulnerability. 	NIST SP800-30
Threat Analysis	The examination of threat-sources against system vulnerabilities to determine the threats for a particular system in a particular operational environment.	NIST SP800-30
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.	NIST SP800-30

2.5 REFERENCES

- NIST SP-800-30: Risk Management Guide for Information Technology Systems.
- ISO 73: Risk Management.
- ISO 13335: Guidelines for the management of IT Security.
- ISO 17799: Code of practice for information security management.
- ISO 15408: Common Criteria.

INTRODUCTION

A New Model for Computer Security Risk Analysis, Capt. Sophie Martel, M.SC. Thesis, Carleton University, Ottawa, June 2002.

ITSG-04 – Threat and Risk Assessment Working Guide, October 1999. The ITSG-04 provides guidance to an individual (or a departmental team) in carrying out a Threat and Risk Assessment (TRA) for an existing or proposed IT system.

2.6 REFERENCE WEB SITES

[W1]: NIST: <http://csrc.nist.gov/publications/nistpubs/index.html>.

[W2]: DCSSI (EBIOS): <http://www.ssi.gouv.fr/document/docs/EBIOS/ebios.html>.

[W3]: NATO: <http://www.nato.int/>.

[W4]: Attack trees: <http://schneier.com/paper-attacktrees-ddj-ft.html>.

[W5]: Spanish RA tool: <http://www.ar-tools.com/en/download/index.html>.

[W6]: CRAMM: www.insight.co.uk.

2.7 SCOPE AND OBJECTIVES

By bringing together experts in a Task Group to:

- Identify existing national methodologies.
- Define main steps for risk analysis with associated tools (without building up a new complete methodology):
 - Identify security needs;
 - Selecting and analysing threats;
 - Selecting and analysing vulnerabilities; and
 - Define security objectives and requirements.
- Study possible links with Common Criteria and related tools.
- Identify techniques to support information interchange using existing tools.
- Identify evolutions to existing methods and tools.

2.8 ACKNOWLEDGMENT

As Chair of the Task Group Jean-Pierre Lebéé acknowledges the substantial volunteer efforts put in by the members of the Group, either in participating to the meetings or by their inputs to the final report.

This report is produced by the following nations:

- Belgium;
- Canada;
- France; and
- United States.

And with the active contribution of NC3A and NHQC3S.