Aruba Cloud

Risk management for information security

CONTENTS

Aruba S.p.A.
Via San Clemente 53 - 24036 Ponte San Pietro (BG) – VAT no.: 01573850516
https://www.arubacloud.com - https://www.arubacloud.fr - https://www.arubacloud.es

1 TERMS AND DEFINITIONS

This chapter contains some definitions considered significant for the representation of the Information Security Risk calculation and management model.

***BIA (Business Impact Analysis)*:**

Analysis of the economic, regulatory and reputational impacts for the Business related to the loss of Confidentiality, Integrity and Availability of information associated with a given process/service and its interruption.

Availability:

Ensure that the necessary information systems and data are available for use when needed.

Risk management for information security

A set of activities and business processes designed to identify, measure, mitigate and monitor the risks associated with the loss of Confidentiality, Integrity and Availability (CIA) of data and services.

Impact:

The negative consequence of the occurrence of one or more threats.

Incident:

A cybersecurity-related event that has a significant likelihood of compromising business operations and threatening information security.

Integrity:

This refers to the protection of data and information from changes in its content, whether accidental or deliberate.

Threat:

The potential cause (deliberate or accidental) of an incident that might damage a system or an organization, generating impacts on the **C**onfidentiality, **I**ntegrity and **A**vailability of information.

Threats may be:

- "Cyber" threats - these have a negative impact on the company by:
  - using the information system or its components (e.g.: attack by hackers);
  - carrying out information system management activities (e.g.: damage by internal personnel);
- "Non-Cyber" threats - these have a negative impact on the company's IT system by:
  - having a direct impact on the delivery of information system services (e.g. natural disasters, interruption of support services);
  - affecting how the information system is managed (e.g. how IT processes are implemented).

To characterize the risks associated with each threat, we need to understand:

- The vulnerabilities of the components of the information system, or where threats may materialize;
- Exposure of the components to the threat, in other words, how easy it is for the threat to materialize (for example, a server that exposes a web service to customers is more exposed to attacks carried out by the internet);
- The types of consequences, considering that some threats can in turn be "vehicles" for other threats (for example, unauthorized access to a web server can allow an intruder to steal data, but it can also allow that data to be deleted, altered, fraud can be committed etc.).

Possibility or probability of occurrence:

The likelihood that a threat may occur affecting one or more IT components, to cause a negative impact to the business, over a period of time.

Information security risk (hereinafter also "risk")

The combination of the probability of a threat occurring and the impact on the company in relation to the assets involved in the analysis. Depending on when they are measured, risks can be defined as:

- Potential or inherent risk (**rRp**):

  This represents the maximum risk that a given asset is subject to in terms of the possibility of creating a threat that can have an impact in terms of a loss of information Confidentiality, Integrity or Availability. All the components involved in the analysis of the service contribute to determining the inherent risk: processes, applications, data, infrastructures and, last but not least, human factors.

  It is basically represented by a value, calculated differently according to which methodology is applied, based on the sum of all the possible threats to which an asset is subjected, considering the respective probabilities of occurrence and their impact.

  In other words, it is the risk to which an asset may be exposed simply because of its nature and the threats associated with it. For example, a computer exposed on a public network without any protective measures.

- Residual or final risk (**rRf**):

  This represents the risk to which a service may be subjected after countermeasures have been applied to reduce the inherent risk.

- Final Acceptable Risk (**rRfa**):

  This represents the maximum risk threshold acceptable to the Organization.

All the risk values set out above are to be regarded as dynamic, because they vary over time, as they are influenced for example by the following elements:

- Evolution of threats;
- Change to the required service levels;
- Changes to legal provisions of benchmark regulations;

- Organizational changes that may affect weaknesses or the likelihood of threats, or change the resulting impact;
- Strengthening or weakening of security countermeasures.

Basic Risks:

This refers to information security cyber risks associated with each asset and each risk scenario.

Confidentiality:

This refers to the protection of data and information in order to mitigate the risks associated with unauthorized access to or use of the information.

RPO (Recovery Point Objective):

This relates to acceptable data loss and is the maximum period of time between the last time the data from a process is saved and the event that causes the process to stop.

RTO (Recovery Time Objective):

The period of time after an incident within which:

- The Product or Service must be recovered, or
- The activity must be resumed, or
- The resources must be recovered.

Risk Scenario:

Combination of two or more threats that allows them to be classified.

Vulnerability:

Inherent weakness of a process, service or asset, which, when exploited by one or more threats, allows Information Security targets (Confidentiality, Integrity and Availability) to be breached. Examples include:

- Non-segregated networks;
- Use of protocols that are not protected by encryption;
- Operating systems not regularly updated;
- Databases with unencrypted "sensitive" data;
- Virus definitions not updated;
- Unmonitored physical access;
- Lack of automatic fire-fighting systems;
- Insufficient backup power systems;
- etc.

2 MAIN REFERENCE STANDARDS

The main standards adopted to make sure that activities carried out comply with international best practices when it comes to security are those described in the following paragraphs.

2.1 ISO/IEC 27001 Standard

The ISO/IEC 27001:2013 standard constitutes is an international security standard and a true benchmark for assessing the level of information security capable of analyzing both the technological and organizational components that contribute to defining an Information Security Management System (ISMS).
The standard defines the requirements for an ISMS and helps to identify, manage and minimise the variety of threats to which information is regularly subjected. This standard also establishes the security controls to be adopted to protect information by making it secure to stakeholders, including the organization's customers.

2.2 ISO/IEC 27002 Standard

The ISO/IEC 27002:2013 standard defines the guidelines and general principles for implementing an adequate Information Security Management System within an organization.
In particular, the ISO/IEC 27002:2013 standard constitutes an international safety standard and a true benchmark for assessing the organizational, procedural, technological and regulatory aspects of the security of an information system in order to:

- Carry out a critical examination of the services and functionalities that the system in question already has or should have;
- Highlight vulnerabilities of the system;
- Indicate the appropriate actions to achieve the level of security defined in the objectives.

It should be noted that ISO/IEC 27002 identifies the security controls that an organization should consider, but does not replace the Risk Analysis itself.

2.3 ISO/IEC 27005 Standard

ISO/IEC 27005 describes the information security risk management process and associated actions, supporting the general principles contained in ISO/IEC 27001.
The standard - in line with ISO 31000 - is intended to help companies manage information security risks in a similar way to how they manage other types of risk.

Figure 1 shows the risk management process proposed by ISO/IEC 27005:11, which inspired the model adopted and developed by the Aruba Group.

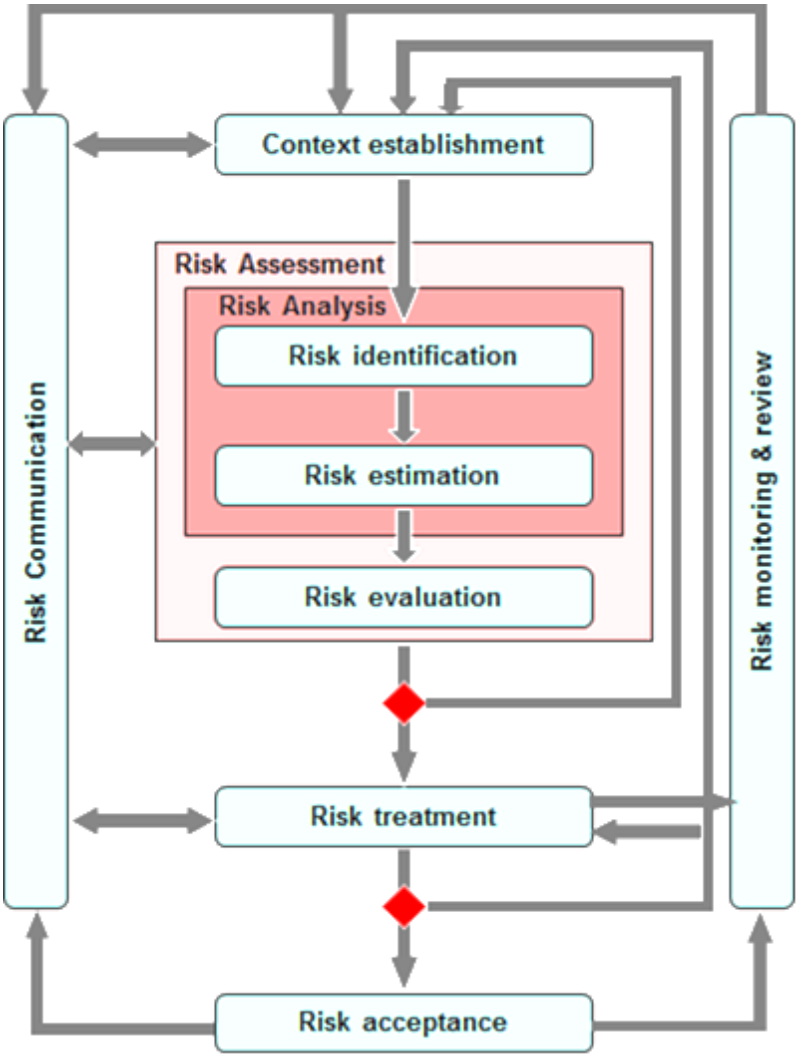

Figure 1 – ISO/IEC 27005: Risk management process

3 METHODOLOGY FOR MANAGING INFORMATION SECURITY RISKS

For the Aruba S.p.A. Group, information represents an asset which requires careful management and is strategic for the protection and development of the company's business.

Against this backdrop, cyber risk can be defined as any uncertain event that could compromise one or more of the following three main properties of the company's information assets:

- **C**onfidentiality (the data is accessible to unauthorized individuals);
- **I**ntegrity (data may be subject to unauthorized modifications and may be altered);
- **A**vailability (the computer system cannot be used);

depending on the level of severity, which is strictly dependent on the type of information impacted.

The risk assessment takes into account the following possible types of impact:

- Economic;
- Regulatory;
- Reputational.

Information security risk management is a process for assessing the interrelationships between assets, threats, and vulnerabilities in an organization. This analytical process is designed to identify the risks associated with the vulnerabilities and threats found in assets and provide the basis for defining an efficient security program.

The risk categories considered must be in line with the types applicable to the context. The risks considered may therefore derive either from internal, external or environmental threats, as well as from deliberate acts or the inadequate organizational management or negligence of individuals.

The value of the risk is understood as a function of the value of the assets in question, the value of the threats and the vulnerabilities.

The results of the risk analysis are documented and include:

- The clear identification of the key risks;
- An assessment of the potential impacts that each of the identified risks could have on the business;
- A plan of recommended actions to reduce the risks and bring them back to an acceptable level.

The Aruba Group establishes a qualitative analysis model, because it can instantly provide a high degree of awareness of the major ICT risks impacting the technological environment in question.

The methodology adopted is:

- Used by the Group in order to estimate the value of the information in the relevant processes and the level of risk to which they are subjected, so that appropriate protective measures can be adopted;
- Also applicable when new infrastructural or application solutions are developed that have an impact on the security of the data being managed. In this case, the methodology makes it possible to assess how critical the data and the threats to which they are subjected are, so that those responsible for risk analysis, when developing and acquiring computer systems, can implement appropriate protective measures to minimize vulnerabilities.

The risk assessment and the analysis of the correlations between assets, threats and countermeasures are carried out with the support of an internally developed tool, using the information collected during specific meetings with the different individuals involved in the processes being analyzed.
The methodology means that a business model can be created where all the basic elements needed for subsequent analyses are described, together with their characteristics, their hierarchical structure and the associated connections.

4 THE RISK MANAGEMENT PROCESS

The main phases of the analysis model for managing risks associated with information security adopted and applied by the Aruba S.p.A. Group are described below.

4.1 PHASE 1 – Context Establishment

The definition of the context for the analysis involves modeling the company's situation and identifying the main business services, processes, macro-processes and assets involved.

When it comes to identifying resources, as suggested by ISO/IEC 27005 “Information Technology – Security Techniques – Information Security Risk Management”, two distinct types are considered:

- **Primary resources** – information, processes, macro-processes and business services;
- **Secondary resources or assets** – hardware, software, personnel, network, location and organization.

4.1.1 Identifying services, processes and macro-processes

When it comes to identifying the Organization's services and processes, the organizational structures published and made available through the internal corporate communication tool are used as the initial references.
Subsequently, the individual processes, which contribute to the provision of services, are grouped into macro-processes specific to the context being analyzed.

4.1.2 Identifying assets

In order to ensure the accurate identification of the assets, we follow these steps:

1. **Identifying the categories** of information assets (e.g. hardware, software, location, etc.), according to the classification system defined within the ISO/IEC 27005 standard;
2. **Weighting the categories** of information assets according to the company's security strategy and business, legal and contractual requirements;
3. **Identifying dependencies** between the categories of the assets that have been categorized.

4.1.3 Parental links between macro-processes and assets

Once the assets have been identified, the dependencies between them and the macro-processes are defined.

These dependencies mean that CIA impact values can be associated with each asset category (determined through BIA interviews), so that the basic cyber risks associated with each asset can be calculated.

4.2 PHASE 2 – Risk Analysis

4.2.1 Assessing impacts

The impact assessment (Business Impact Analysis) is carried out in accordance with the method adopted in addition to the main international standards (ISO 27005, ISO 22301), by Business representatives.
During the BIA interview phase and using a tool developed internally to collect information, the Managers of the different company departments assess the loss of Confidentiality, Integrity and Availability of the information managed within their area of competence in terms of economic, regulatory and reputational impact, according to well-defined assessment scales.

As specified in PHASE 1, individual processes are grouped into macro-processes specific to the context being analyzed. The impacts associated with these macro-processes are calculated as the *"worst case"* of the individual impacts of the different processes that make them up.

4.2.2 Identifying and valuing assets

The identification of assets is the starting point without which it is not possible to manage a company's security properly and effectively. The inventory is in fact the starting point for classifying the company's assets and for analyzing the level of risk to which they are subjected.

The purpose of this operational phase is to draw up an inventory of information assets, or formalize existing methodologies for this, considered by the company to be "mission critical" in order to achieve its business objectives, to comply with its contractual obligations and, lastly, to comply with the rules and legislation to which its activities are subject.
The central value of an asset is usually represented by the information (or data) that the system processes, leaving the task of processing or protecting them to other assets.
Within this context, the value is assigned, during the BIA interviews, for each asset and for each of the CIA dimensions (confidentiality, integrity and availability) of security applicable to the context.

By using the information collected during the interviews, it is therefore possible to associate the impacts deriving from the macro-processes in which they are used with each asset.

4.2.3 Analyzing threats and assessing their probability

The methodology used in the information security risk management process defines a timely step in determining the threats that affect the assets in question. Threats represent all those elements or events that can cause damage to an asset.

The purpose of this activity is to identify the threats and vulnerabilities affecting the assets identified and included in the risk analysis and management process and to assess the likelihood of their occurrence.

To make sure the list of threats is exhaustive, reference is made to the list of threats in the ISO/IEC 27005 standard, in addition to the considerations produced and published by ENISA following its studies on the subject.

The individual threats are subsequently grouped into realistic risk scenarios for the context under analysis.

4.2.4 Analyzing countermeasures

The purpose of this activity is to identify the countermeasures deemed necessary to cover the risk scenarios for the assets identified in the previous step.

To make sure the list is exhaustive, the Aruba Group S.p.A uses a list of countermeasures based on the best practices of the ISO/IEC 27001:2013 Annex A standard. Depending on the type of service analyzed, assessments can be enriched for specific subjects by analyzing further checks suggested by authoritative sources, such as ENISA, AgID, NIST, etc.

Once the list of security checks has been defined, they are mapped with respect to the risk scenarios, on which they can be carried out to reduce the probability of the relevant threats occurring or their impact.

The counter-measures have been divided into:

- **Reactive** (r), designed to reduce the impact;
- **Preventive** (p), designed to reduce the probability of a threat occurring.

4.3 PHASE 3 – Risk Evaluation

4.3.1 Risk model and methodology

The value of the risk is understood as a function $R = f(A, M, V)$, with A the value of the assets in question, M the value of the threats and V the vulnerabilities.

Through PHASE 2 of the information security risk management process, the risk model can be defined (*Threat Modeling*). This is a process used to identify potential threats and vulnerabilities, assess how likely they are in a specific circumstance, put them in order of priority, and reduce the risk of them occurring by implementing appropriate countermeasures.

Once the basic context has been defined, the *Threat Modeling* process involves:

- Making a list of potential attacks/vulnerabilities that includes ways in which the Confidentiality, Integrity, and Availability of data might be compromised;

- Assessing the most likely attacks/vulnerabilities, discarding those that are unlikely or in any case almost impossible to remedy, and for all the others applying controls, or countermeasures that might be technical or procedural.

4.3.2 Applicable security requirements and level of compliance

Once the security requirements deemed to be applicable within the context of the analysis have been identified (see section entitled "Analyzing countermeasures"), the extent to which the requirements relating to the 14 areas identified in the ISO/IEC 27001:2013 Annex A standard are covered is assessed.

The extent to which each countermeasure is compliant is expressed according to a well-defined scale of values ranging from 0, meaning there is no countermeasure, to 4, where the countermeasure is fully implemented.

In order to analyze the level of compliance of the controls required by Annex A of the ISO/IEC 27001:2013 Standard, the information and evidence collected through specific assessment activities conducted internally are used.

4.3.3 Calculating inherent and residual basic risks

During this phase, the value of the inherent and residual basic CIA security risks (AS-IS, Planned and TO-BE) associated with the service under analysis is calculated.

The inherent basic risks for each asset and for each scenario, associated according to the logic described above, are calculated by taking into consideration the probability of individual risk scenarios occurring and the potential impact that they could have.

Once the inherent risks have been determined, to obtain the residual risks (AS-IS, Planned and TO-BE), the values associated with the security countermeasures needed to counter the identified risk scenarios, during the internal audit phase, are taken into account, both in terms of reducing the probability of the threats, and in terms of reducing the impact.

4.4 PHASE 4 – Risk Treatment

4.4.1 Analyzing accepted risks

One of the concepts that must be addressed when it comes to risk management is that of accepted risks. This term generally refers to those risks that for some reason cannot be dealt with conveniently or at all and that are simply accepted.

The purpose of this activity is therefore to define a criterion according to which threat-asset pairs that involve a low risk can simply be accepted. Beyond individual cases, therefore, a threshold is defined below which a certain risk is simply considered a cost and is therefore not dealt with.

4.4.2 Results of the analysis: residual AS-IS risk

The work involved in analyzing and assessing risks, taking into account the countermeasures applied (residual risk), is carried out by implementing the following:

- Assessing security checks with respect to the best practices of Annex A of ISO/IEC 27001:2013;
- Analyzing the impact of the loss of information availability, confidentiality and integrity for the services in question;
- Analyzing vulnerabilities and threats to assets;
- Assessing the as-is information security risk and identifying an order of priority.

4.4.3 Gap analysis and selecting which countermeasures to implement

Following the analysis work carried out, in order to address any relevant risks/issues within the scope of the services provided by the Aruba Group S.p.A. and with a view to pursue the continuous improvement of the ISMS, the data obtained from the analyses carried out in the Risk Analysis tool are processed to identify the risk areas for which appropriate security measures need to be defined.

To identify the actions deemed necessary to improve and reduce risks, a gap analysis is therefore defined, from time to time, designed to assess the discrepancy between the current level of application of security countermeasures and the maximum applicable level.

4.4.4 Risk Treatment Plan - Rationalizing intervention

The actions identified in the gap analysis are then grouped into specific project initiatives and documented within the Risk Treatment Plan.

5 FREQUENCY OF ANALYSES

The information security risk management process shall be completed every 12 months, or sooner if there is a significant event, including, but not limited to:

- New assets that come under the scope of Risk Management;
- New threats both inside and outside the organization that have not been assessed;
- The possibility that new or increased vulnerabilities may be exploited by threats;
- Review of vulnerabilities already identified to determine those that may be more exposed to new or re-emerging threats;
- Increased impacts or consequences of threats on assets, vulnerabilities and risks that together result in an unacceptable overall level of risk;
- Particularly serious security incidents.

In addition, analyses may be carried out at different frequencies, for example in relation to compliance with particular standards or certification requirements.