International Journal of Engineering Science Invention (IJESI)
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org ||Volume 7 Issue 10 Ver V || Oct 2018 || PP 36-47

Study and Design of Risk Assessment Procedure and Basic Penetration Tests before the Production Environment

D.Kasinas[1], C.Drosos[1] and D.Tseles[1]
[1]*Department of Industrial Design and Production Engineering, University of West Attica, Greece*
Corresponding Author: D.Kasinas

Abstract: *This work attempts to capture and present the basic actions required to organize the security of the IT systems of an organization. Initially analyzed security audits based on the OWASP testing project, provides guidelines for the proper development of a comprehensive information security framework. An effort is then made to develop an information security risk assessment methodology, as well as a policy of identifying weaknesses and conducting security audits. Finally, penetration tests are run on a web application in order to detect any security problems before it enters production. Tests are performed using the OWASP Zed Attack Proxy (ZAP) tool.*

Keywords -*Information Security, Risk Assessment methodology, Vulnerability Tracking Policy, Penetration Testing*

Date of Submission: 17-10-2018 Date of acceptance: 03-11-2018

I. Introduction

The rapid development of Information Technology has resulted in the construction of products throughout the everyday human life. Public and private companies and organizations, through the development of their information systems, managed to increase their production processes and offer better products and services that were virtually impossible to implement before the explosion of Information Technology.

Nowadays, the overwhelming majority of organizations rely on IT for its daily operations. Any potential problem in information systems results in the delay or even interruption of organisms as long as it lasts.

However, with the rapid development of IT and the benefits it brings to the lives of people and businesses, at the same time of delinquency is developing aiming at the interception of sensitive elements or the creation of cybercrime problems.

In order to address the above threats, organizations are now obliged to organize their protection in order to defend them in cyber attacks.

It is understandable that the more critical the sector in which an organization is deployed, the more complex the procedures are used to protect it, whereas the necessary vulnerability checks are necessary to be carried out at regular intervals or at each change of the system. Nowadays, large organizations have developed systems of continuous monitoring of the security of their IT systems, as well as privacy and security by design.

However, how can an organization estimate the cost of a possible attack on its information systems, whether the loss is related to money costs (e.g. revenue cuts, criminal proceedings, fines from regulators, loss of data, etc.) or even costs his reputation (for example, a decrease in confidence in the organization, downgrading of a trade name, etc.)?

It should be noted that the cost of a security incident may vary depending on the type of attack and the rate of success. To this end, it is necessary to calculate the effect of a possible attack by conducting a risk assessment using methodologies and standards to allow for the identification of the security investments required for an organization. This calculation needs to be evaluated and reviewed annually.

II. Security checks based on the OWASP Testing Project

OWASP is a global free community and also one of the most widespread standards for software security. OWASP has been developing for many years the OWASP Testing Project, which aims to help understand web application testing.

A security measure parameter, apart from the technical issues that relate to, for example, how widespread a particular vulnerability is, is also the calculation of the impact of security issues on the total cost of the software. Although most technicians are able to manage and address the vulnerabilities of an application, unfortunately a very small percentage of them is able to estimate the possible impact of vulnerabilities in the business activities applied by the application. This parameter causes problems for organizations' IT officers who

have difficulty capturing the exact return on security investment, as well as compiling their respective budgets for software security.

Based on the above, it seems important to be able to evaluate security throughout the development process and then estimate the cost of unsafe software to the impact it may have on the business. This will lead to the development of appropriate business processes and allocation of resources for risk management.

A proper method of preventing the occurrence of security failures in production applications is the improvement of Software Development Life Cycle (SDLC), where security is integrated at each stage. An SDLC is a structure that is required to develop software objects.

The SDLC model which is preferred should ensure that security is an integral part of the development process. Safety tests should also be included to ensure that safety is covered and controls are effective throughout the development process.

2.1. PRINCIPLES OF SECURITY TESTING

An application security evaluation software cannot succeed in-depth assessments as well as provide adequate coverage of the tests, by estimating that safety is a process and not a product. In order to avoid the occurrence of recurring security problems in an application, it is appropriate to create a security applied to the Life Cycle Software Development.

By integrating security into all phases of the Software Development Lifecycle, an overall approach to application security is achieved, taking advantage of the organization's existing processes.

The existing Life Cycle Security Frameworks provide descriptive or guidance tips. Depending on the maturity of the procedure followed in the organization, the corresponding version of the security frame is also selected.

It is understandable that when a bug is detected as quickly as possible in the Software Development Lifecycle, it is treated accordingly faster and at a lower cost. To achieve this, it is important to be as safe as possible on security issues, development teams and audits. It is also important to know the security required for the project, based on its classification in order to handle it properly (confidential, secret, top secret, etc.).

A successful vulnerability test for an application requires the test to be done using "out of the box" logic so that the security test is not done based on the normal behavior of the application but on the behavior of an attacker attempting to break an application. Given that each application is deployed in a unique way, even if common application development frameworks are used, automated security checking tools often fail in controls, because checks should be performed on a case-by-case basis.

Therefore, it is important to initiate a security audit as soon as possible, making the best possible documentation of the application, such as architecture, flow charts and usage cases.

The completion of a test procedure, is important to include a log file that records the test actions, the users and the results of the tests. The format of the report should be structured in an understandable way for all the persons involved.

2.1.1. Security Test Techniques

A control technique is used to implement a security testing program. Based on the OWASP Testing Guide [1], these techniques are:

- Manual Inspections and Review
- Threat Modeling
- Code Review
- Penetration Testing.

2.1.2. Selection of the best technical safety tests

The best approach in order to select the right technique involves a balanced use of various techniques that will cover the testing at all phases of the Software Development Life Cycle, utilizing the most appropriate techniques per development phase. A balanced approach varies from case to case and depends on many factors such as the maturity of the testing process or corporate culture and policy.

2.2. IMPLEMENTATION OF SECURITY TESTING REQUIREMENTS

Security requirements determine the objectives of a test program. The main objective of the safety tests is to validate the expected operation of the controls through safety requirements. This means ensuring data and service, availability, confidentiality and integrity. On the other hand it is also crucial to validate the implementation of security controls with as few vulnerabilities as possible.

Initially, an understanding of the business requirements is needed to document the security requirements respectively.

The main objective of the safety tests is the validation of safety requirements in terms of functionality. Accordingly, based on risk management, the objective of the information security assessments is to fulfill the safety requirements.

Based on the safety assessment, safety requirements are validated per Life Cycle Software Development Cycle, using different testing techniques and methodologies. An important factor in verifying that security controls have been designed and built to mitigate the impact of vulnerability exposure is to take into account the underlying causes of these vulnerabilities based on the classification of threats and countermeasures.

2.3. PROVISION OF FUNCTIONAL AND NON-FUNCTIONAL TEST REQUIREMENTS

Standards, policies and regulations applied to an organization create the need for security controls and control functionality. The security requirements are divided into "positive requirements" and "negative requirements".

"Positive requirements" concerns the test of expected functionality through safety tests. By testing the positive requirements, the expected functionality is confirmed according to predefined inputs.

Respectively, the "negative requirements" refer to security tests that control unexpected behaviors.

2.4. SECURITY TESTS EMBEDDED IN DEVELOPMENT AND TESTING WORKFLOWS

By integrating security testing into the Software Development Lifecycle, developers are enabled to control the individual components of the software before integrating with other components and joining the deployed application. Software components, to be tested may consist of software objects such as functions, methods, classes, interfaces, libraries, or executable files.

Given that during the workflow of the software development process, data and code changes are tested by developers the applications change and finally testing is required in the application as a whole.

2.5. DEVELOPER SECURITY TESTS

The main purpose of security testing for a developer is to validate that the code has been deployed according to secure encoding standards. Coding tools, such as functions, methods, classes, APIs and libraries, must be validated before being embedded in applications.

2.6. SAFETY FUNCTION TESTS

Integrated System Testing is intended to validate that the implementation of security controls provides multilevel security protection.

2.7. ANALYSIS AND REPORTING OF SECURITY DATA

The definition of safety measurement objectives is a basic requirement for the use of safety trial data for risk analysis and risk management processes. The whole amount of security test findings, for example, can lead to quantification of the security level of the application. They can also help to identify the objectives of software security testing, such as setting the minimum acceptable number of vulnerabilities before the application enters production.

It would also be possible to compare the security level of the application with respect to a certain minimum security level in order to assess the safety procedures.

The security level of an application is characterized by the visual aspect of the result, such as the number of vulnerabilities and their risk assessment, as well as their causes or origins, such as coding errors, architectural defects, and configuration issues.

Findings can be classified according to different criteria, such as the Common Vulnerability Scoring System (CVSS) of the Forum of Incident Response and Security Teams (FIRST) [2].

A safety test data report, based on best practice, should include the following information:

- Categorizing a finding
- What is threatened by the finding
- The main cause of security issues
- The control technique used
- The recommended countermeasures
- Scoring the criticality of the finding

III. Risk Assessment Methodology

Assessing information security risks is very important for an organization because it aims to identify and manage the risks to the security of its information resources. An information resource is defined as a service, application, system or network where valuable information from the organization is processed or transmitted.

To this end, it is appropriate to have a methodology for assessing information security risks. This methodology can help the organization to comply with regulatory requirements as well as help to make decisions that align actions and investments with the level of risk acceptable to the organization and is defined as tolerance risk.

This methodology will aim to set a framework that can continually recognize, assess and monitor information security risks. It will also be able to define the appropriate security measures. The auditor (or auditing team) will be able, through the risk assessment methodology, to:

- Recognize critical information resources for the organization's operations and strategic goals
- Recognize and assess whether it is probable that any vulnerabilities or vulnerabilities existing in the security locks may be used by threats
- Estimate the potential risks that have financial or even non-financial effects
- Identify and classify the risk profile that threatens information resources with a view to implementing an appropriate plan to control these risks
- Proposes appropriate techniques that will be able to identify and prevent the sources of threats that will attempt to exploit vulnerabilities in order to limit the risks to acceptable levels
- It is able to continuously monitor and report the identified security risks.

A risk assessment methodology should be able to support:

- Critical information systems and organization information
- New systems ready for production, whether purchased or developed internally in the organization
- Existing information systems that have undergone significant changes or updates
- Any new products, services, or processes that have been developed
- Application of new technologies (e.g. cloud networks, virtualization, wireless networks etc.)
- Existing or new external partners and / or suppliers who provide critical services.

3.1. OVERVIEW OF THE METHODOLOGY

The information security risk assessment methodology consists of processes, practices and tools that will determine the control, management and evaluation of information security risks and are designed to provide the necessary assistance to the auditing group so that it can implement a safety risk assessment.
Figure 1 outlines the steps of the information security risk assessment methodology.

Stage 1: Start and Scheduling

Prior to a major change in facilities, operations or technological change, it is considered necessary to carry out a risk assessment. It is also required to be implemented after a major security incident or in cases where a new significant risk arises or even a new regulatory requirement. In addition, there should be a periodic risk assessment plan for the organization's critical operations.

For the need to carry out a risk assessment, the security officer is notified by the person in charge of a department, installation or project. An Information Security Officer may also trigger an evaluation if a hazard area is identified through the continuous monitoring of security threats.

The steps taken to accept and approve the project plan of an information security risk assessment are analyzed below:

- Identify the main assessment team
- Confirming the scope of the information security risk assessment
- Organization of Project and Arrangement Management Approach
- Update the Evaluation Team and start the evaluation
- Acceptance and approval of the project plan.

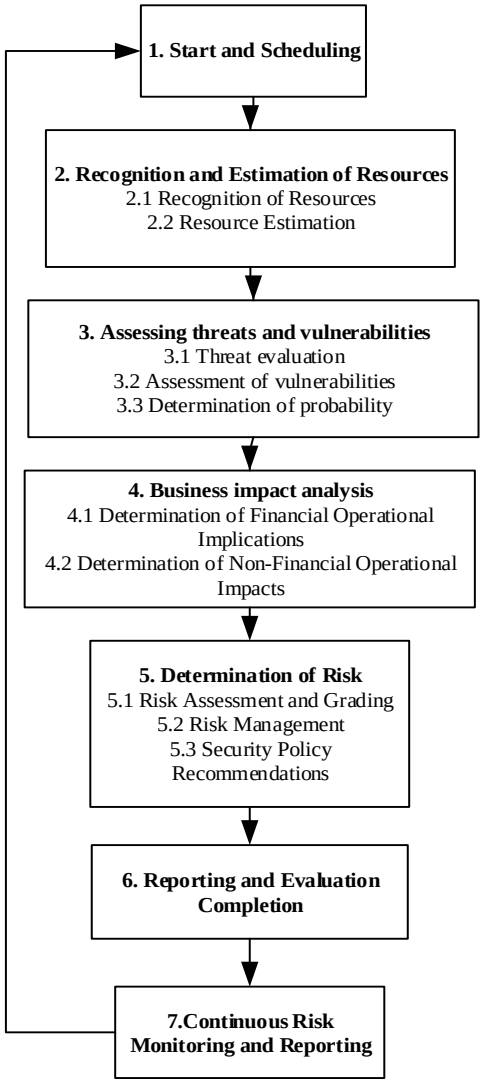

Figure 1: Stages of the methodology

Stage 2: Recognition and Estimation of Resources

The next step will be to identify the critical processes and information resources of the organization that will be integrated into the information security risk assessment process.

The choice of critical processes only needs to be done as it is not always effective to carry out a risk assessment of an organization's entire information technology resources.

The two crucial actions of this phase are "resource recognition" and "resource assessment".

The term "resource information" may have a very range of an application. For this purpose, in an information security risk assessment process, information resources represent any informational asset or set of informational goods supporting the organization's processes.

Stage 2.1: Recognition of Resources

The evaluation team will initially recognize the information resources at a satisfactory level of detail, from the operational process or a single system perspective, in order to assess these resources.

The evaluation team collects process and resource data in order to carry out the risk assessment. To make resource recognition, a collection of data from various sources is conducted, such as relevant interviews.

If the evaluation team follows a process-based approach, it must analyze the process and then decompose it into logical components of evaluation or resources.

Stage 2.2: Resource Estimation

Once the information on the relevant process and information resources has been collected and has been structured into sensible evaluation components, each component has to be assessed based on the level of criticality. The value of the resource is derived from the level of classification of the information or the information system defined in the actions of Stage 2.1 and results in a rating scale according to Table 1.

Table 1: Resource Estimation Decision Table

ResourceRating	Continuity with Risk Assessment?
Critical	**YES**
Sensitive	**YES**
Non Critical	**YES/NO**

The assessment of the value of the resource should be consistent with a corresponding "Information Resources Grading Methodology". The assessment of the value of the resource ultimately determines whether the Evaluation Team will continue with the information security risk assessment process for an information resource.

Stage 3: Assessing Threats and Vulnerabilities

The threat and vulnerability assessment process checks the possibility of occurrence of incidents that may compromise the confidentiality, integrity or availability of the organization's information. By fully controlling the various combinations of threats and vulnerabilities associated with an information resource, the assessment team will be able to have a clearer understanding of the frequency and exposure of specific incidents to be exploited by the corresponding sources of threats.

Stage 3.1: Threat evaluation

The range of threats that may compromise the confidentiality, integrity and availability of the organization's information is large. Threats may arise from inadvertent human errors or dysfunctions of supporting infrastructure, or even deliberate attacks from malicious third parties.

It is most likely that it is not always possible to carry out an assessment in a system that takes into account all possible threats. It may not be practical in many cases. To this end, it is appropriate for the project to identify a list of threats to be used to assess threats, which should be realistic and manageable.

For the purpose of conducting an information security risk assessment process, a threat is divided into two main elements:

The threat agent: refers to the source of the threat
The threat action: refers to the actual action being taken by the threat.

Stage 3.2: Assessment of vulnerabilities

The vulnerability assessment process involves assessing the level of vulnerabilities and the effectiveness of security controls associated with an information resource. The existence of vulnerabilities or vice versa weaknesses in security controls increase the likelihood of a threat agent to exploit vulnerability and achieve the associated threat action.

Initially, the assessment team should evaluate the effectiveness of the existing safeguards for each identified threat and choose the rating value. This can be achieved through the use of various existing data and information sources by information owners and specialists with object managers using indicative lists of vulnerabilities.

At this point, it is necessary to decide or calculate if the level of risk is acceptable, so the assessment of the safety valve is "Strong" or "Sufficient", taking into account the existing measures. If this is the case, then the security risk assessment process is completed. Otherwise, the information security risk assessment process is continuing for the relevant threat.

Stage 3.3: Determination of Probability

As a probability, in the framework of the information security risk assessment process, the estimated frequency (likelihood of occurrence) where a threat may exploit a vulnerability or vulnerability that has been identified, and thereby adversely affects the confidentiality, integrity or / and the availability of the information resource.

"Frequency" is the price that the Assessment Team will set to indicate how often an incident is likely to occur. For each risk, the Review Team will calculate the frequency value. Impact and frequency assessment is more subjective than accurate.

Therefore, all available sources of information, whether internal or external, should be exploited to minimize the subjectivity inherent in the information security risk assessment process and to ensure the consistency of risk assessment.
The frequency and impact factors to be taken into account, and the sources of information are as follows:

- Older issues or findings
- Key Risk Indicators (KRIs)
- Data Loss (Internal Sources) / Older Events
- Data Loss (external sources)
- Existing Safety Drivers
- Operational Environment Factors
- Expert Opinion and Judgment
- Other factors worth mentioning

Stage 4: Business Impact Analysis

Business Impact Analysis is a process based on business operations and aims at assessing the impact (financial and / or not) that is expected to be caused by compromising the confidentiality, integrity and / or availability of an information resource that is due to the successful exploitation of a vulnerability from a recognized threat.

The value resulting from the Business Impact Analysis (or risk analysis) reflects the cost of the impact of the risks on financial and / or qualitative terms.

The operational impact (or the impact of the risks) is measured in financial and / or non-financial terms.

Since Business Impact Analysis is an operational activity, the information provided by Information Managers and related business personnel is critical.

Stage 4.1: Determination of Financial Operational Implications

Financial impacts can be assessed at two levels:

- Average Value
- Maximum Value

The determination of both "Average" and "Maximum" value is done using standard scales of impact rather than individual values.

Stage 4.2: Determination of Non-Financial Operational Impacts

At this stage a Repeat of Stage 4.1 actions should be performed for each identified risk in relation to the Non-Financial Impact using a relevant table where the highest incidence per qualitative class is selected.

Stage 5: Determination of Risk

At this stage, the results of Frequency, Financial and Non-Financial Impact for each risk are combined and matched to produce an overall risk assessment. The overall risk assessment is reflected in a range of four values:

1 – Low Severity	2 – Medium Severity	3 – High Severity	4 – Critical Severity

Figure 2: Risk assessment rates

According to the results of the Risk Assessment, every risk is assigned to a risk map (Financial or Non-Financial). The risk map sets out the categories of risk and frequency effects, where each grade is actually a range of values. The product of the loss value and the probability value gives an average value of the expected loss from a probable event and represents the residual risk.
The risk assessment will ultimately determine the risk management actions.

Stage 5.1: Risk Assessment and Grading

At this stage, for each identified risk, an overall Frequency and Total Financial and Non-Financial Impact Assessment should be mapped. The work is repeated for the other dangers.

Stage 5.2: Risk Management

In this step, the Assessment Team has adequately understood the information security risks of information resources and is ready to examine the response to the risk or the options to address them. The objective of this step is to select an appropriate risk response or action to achieve an acceptable level of residual risk that is in line with the organization's tolerance requirements.

Overall, there are four (4) broad categories of risk response:
- Avoid
- Decrease
- Sharing / Transfer
- Accept

If the overall risk has been assessed as "Medium", "High" or "Critical", then a risk plan for risk action is required. If it has not been evaluated with one of the above categories, then the process is terminated for that particular risk.

Stage 5.3: Security Policy Recommendations

Where risk management has been selected through risk reduction, the Assessment Team should propose appropriate safeguards to effectively reduce the likelihood of the threat source exploiting the vulnerability to an acceptable level of residual risk.

Choosing the right safety valves requires a good understanding of the safety valves available to meet a particular requirement within the organization, knowledge of how they work, and how effective they are under the circumstances.

Stage 5.4: Risk Management Plan

Final work at this stage requires the unification and prioritization of selected risk decisions by the Assessment Team. The risk management plan shall include the essential characteristics of each hazard identified on the basis of the data collected, the calculated values and the safety guides proposed to reduce the risks to an acceptable level.

Any risk also requires the identification and assignment of a risk holder who will be responsible for reviewing and approving risk plans and other risks. The Risk Owner will also be responsible for the implementation of the risk plan.

Stage 6: Reporting and Evaluation Completion

The goal of this phase is to finalize the deliverables and complete the information security risk assessment task. At the end of this phase, the Evaluation Team will have communicated the results of the risk assessment to all relevant stakeholders and will have collected all the 'working documents' needed to support all activities carried out in the safety risk assessment process information. It is important that the working papers and all the information used are maintained, as the results of the risk assessment are subject to review by the same stakeholders, auditors or regulators.

Stage 7: Continuous Risk Monitoring and Reporting

The primary objective of this phase is to ensure that the state of risk plans are regularly monitored and key stakeholders are informed. During the security risk monitoring, key stakeholders should be informed of the progress of the agreed implementation actions, the effectiveness of the selected safety measures / actions and the potential areas where improvement or escalation is required to resolve any issues.

3.2. QUALITY ASSURANCE

The following criteria are set to ensure that the quality of the Information Security Risk Assessment process is maintained at a satisfactory level. This will ensure that the analysis is done with valid and accurate data, limiting any future events.
- Effective project management
- Commitment of Project Support and Team Leader
- Commitment of Stakeholders
- Common language / common evaluation criteria
- Regular review of ratings
- Employees training
- An Assistant Risk Assessment Tool
- Quality of Documentation.

IV. Vulnerability Tracking Policy and Penetration Tests

Each organization should aim at creating a policy that will be able to maintain an adequate level of security. The implementation of this policy will help provide information security assurance and will also help assess their security level. Implementation of the policy should be valid at administrative as well as technical level.

For policy making, account should be taken of the key principles of identifying weaknesses as well as the process of conducting audits, the frequency with which security controls will be carried out, the range that they will have, the tools to be used, and how the results of the security controls will be presented and managed.

4.1. BASIC PRINCIPLES

The Information Security Officer, in collaboration with the IT Officer and the Internal Audit Officer of the organization, will be responsible for creating and maintaining a Security Plan. This plan should be checked and reviewed annually.

As soon as the Security Plan is completed will be presented by the Information Security Officer for approval by the organization's management.

Standards under which security and administrative controls will be conducted will be maintained and updated under the responsibility of the Information Security Officer. These standards should include at least the following:

- Control Plan Template
- Audit and Management Information Review
- Summary Template

For outsourcing assignments to implement Security Checks, it is appropriate to have a relevant policy that defines the methods of selecting and managing collaborations with external partners.

All security checks should be recorded in a log life containing the audit data, the results recorded, the corrective actions proposed, and the corresponding actions finally taken to resolve the audit findings. The file manager is the Information Security Officer.

4.2. SECURITY CHECKS

It is important that the number of checks that take place ensure that the organization's security is as effective and comprehensive as possible. Technical security controls should take place for IT systems and infrastructures such as databases, applications, networks, etc., and technical controls of the Internet's security infrastructure, the internal network of the organization, and the protection against malware.

These checks will ensure the effectiveness of the security mechanisms, compliance with the security framework of the organization, and the disclosure of any security weaknesses in order to take appropriate action to correct them. Security Vulnerability defines the absence or failure of a security mechanism that would put an attack on an information system as a risk.

Controls should also be carried out to ensure compliance with the safety management mechanisms implemented by the organization to assess the efficiency of security procedures and standards, to verify compliance with the security framework and to confirm that the implemented security framework covers any organizational and procedural changes that are or may be in relation to its previous audit.

It is understandable that the most important controls carried out in an organization concern the control of the organization's interconnection infrastructure over the Internet.

For the design of controls, formal standards should be calculated and as many as possible or at least the most important of the known scenarios of attacks should be included. At the same time, the procedures for operating and managing the system under review should be checked and evaluated. The purpose of the audit should be recorded and agreed with the operational manager of the application or infrastructure under consideration.

Important factors to be taken into account are the ability of the staff to carry out the audit, its objectivity, and the compliance with the standards and procedures of the organization.

4.3. FREQUENCY AND RANGE OF SECURITY CHECKS

It is important, with a view to assessing the compliance and effectiveness of the security technology mechanisms, and the corresponding administrative mechanisms, that periodic independent safety checks be carried out on these mechanisms in a production environment. Indipended Security Audit defines security controls performed by a mechanism, internal or external, which has nothing to do with the controlled system.

For the design of these security controls, any modifications to the IT infrastructure, organizational infrastructure, technological developments, findings of previous audits, as well as any modifications to the acceptable levels of risk for the controlled infrastructure, should be considered.

The classification of the information system or infrastructure, as well as its risk, determines the periodicity with which the independent audits will be carried out.

A policy, a process or a standard (which are essential components of the organization's Security Information Framework) that have been applied to an organization should be evaluated periodically, with the frequency and range of ratings being proportional to their degree of maturity and their application to the organization.

The assessment of the Information Security Framework should include the following:

- Level of application and competence of information security policies, processes and standards, from the organization's executives, as well as from external partners
- Proficiency level and testing of the Business Continuity Plan as well as the corresponding Disaster Recovery Plan

A plan of periodic technical security controls for the integrated IT systems of the organization should be drawn up, and exceptional checks may be carried out if deemed necessary on the basis of the criticalness of such systems.

The Information Security Officer, in collaboration with the IT Officer, should frequently review the list of IT systems and infrastructures, as well as the plan of periodic inspections, to ensure their adequacy and completeness.

Technical security audits are designed to assess the security technologies used and to ensure that the highest possible level of safety is provided based on their characteristics. The frequency and scope of these checks should be tailored to the requirements.

4.4. USAGE OF SAFETY TECHNICAL INSPECTION TOOLS

Specific software and devices used to perform technical controls must be accessible to a limited number of authorized executives designated by the IT Officer of the organization with the approval of the Information Security Officer.

The tools, used in a technical inspection should be carefully adjusted so that functions that are not required to carry out the check remain inactive.

During a technical inspection, the users of the tools should record all the actions taken, for reproduction and control if required.

4.5. RESULTS OF SECURITY CHECKS

When a security check is completed, the results of the checks are recorded. The results of the security checks are defined by the information recorded by the control. The format of this information can be in documents, archives, source code, etc.

The results of security audits should provide as much information as possible so that the validity of the conclusions and suggestions can be checked also by an auditor that is not related to the audit.

The results of the checks shall contain at least the following information:

- The purpose and objectives for which the security check was carried out, the scope of the audit, the source of the information gathered, the methodology followed and the possible sampling criteria used.
- Documentation of the work done, including the conclusions and proposals submitted. In addition, descriptions of the information systems and infrastructures tested should be included.
- Confirmation of both the completion of the work and its documentation have been accepted by the security officer.

The classification of the information related to the results of the security checks should be done at the corresponding rating level defined by the rating scheme designated by the organization. The results of a security check should be classified at least with a "CONFIDENTIAL" rating.

The results of a security check are delivered by the security auditor solely to the organization's Security Officer and the Controlled Unit Manager.

On the basis of the procedure for correcting the safety deficiencies to be followed, after completion of the modifications, a confirmation check will be carried out, where the methodology and parameters to be followed will be similar to those of the initial safety check, incorrect (non-homogeneous) comparisons.

V. Carry out penetration tests

This chapter will perform penetration tests of an application, the development of which has been completed and is ready for User Acceptance Test (UAT).

Given that previous chapters analyzed security safety recommendations provided by OWASP, it was considered appropriate to use the tool provided by OWASP Zed Attack (ZAP) to perform penetration testing.

5.1. ESSENTIAL FOR PENETRATION TESTING

The penetration tests (Pentesting) is implemented with the controller acting as a malicious external attacker who aims to enter the system and either steal data or perform some kind of denial-of-service attack.

Penetration testing has the advantage of being more accurate because it has fewer wrong results (results that indicate a vulnerability that is not actually present), but it may be time consuming to implement it. It is also used to test defense mechanisms, check response plans, and confirm compliance with security policy.

Automated penetration tests are an important part of the continuous security screening process. They help in discovering new vulnerabilities as well as re-emergence of previous vulnerabilities in an environment that is changing rapidly.

5.2. THE PENETRATION TESTING PROCESS

Both automated and manual penetration is used, often in combination, to test everything in an infrastructure such as servers, networks, devices, and endpoints. In the example to be implemented in this study, penetration tests will be conducted for web application, in a test environment that consists of the absolutely necessary infrastructure, in a virtual environment that has nothing to do with the productive one.
Penetration tests typically follow the following steps:

- Explore - The controller attempts to learn about the system being tested, where it determines which software is used, which endpoints exist, which patches are installed, etc. Also looking for hidden content on the site, known vulnerabilities and other signs of weakness.
- Attack - The controller attempts to exploit the known or suspicious vulnerabilities to prove they exist.
- Report - The auditor reports test results, including vulnerabilities, how they were exploited, and how difficult it was to exploit and sever it.

The ultimate goal of penetration testing is to investigate vulnerabilities so as to address them. They can also verify that a system is not vulnerable to a known category or a specific defect, and in cases of vulnerabilities that have been reported as corrected, they assert that the system is no longer vulnerable to these vulnerabilities.

5.3. TEST ENVIRONMENT

To perform a penetration test, a test environment was prepared which includes a terminal on which Hyper-V Manager was activated. Hyper-V enabled a virtual machine on which Windows Server 2012 R2 was installed. The virtual server has enabled Microsoft IIS 8.
Also in the same virtual server was installed Data Base, Microsoft SQL Server 2012.

The application to be tested has been deployed with Web Forms in the .NET Framework. The test is completed after the application development has been completed, in order to find possible security findings before being given User Acceptance Test (UAT).
To implement the tests, OWASP ZAP 2.7.0 was installed on the terminal where Virtual Server was activated.
Application testing was performed using ATTACK Mode.

5.4. REPORT

The information displayed on the ZAP screen also allows the application to be exported in the form of a report, which provides detailed information per finding, in order of risk category. Each finder provides information such as the description of the finding, the URL in which it was found, the method used with the corresponding parameters, as well as resolution instructions and internet referrals, with additional instructions on each finding and its methods of solving.

The reference to the way it is exported is very important because it provides the most of the information that will need to be given to the stakeholders analyzed in the previous chapters (administration, security officer, IT administrator, etc.) in order to proceed with the actions required to resolve or accept the risk in the event that a finding is deemed not to be solved or its resolution is unprofitable in relation to the risk arising from the particular finding..

VI. Conclusion

Corporate Information is probably the most valuable asset for many organizations. To this end, its protection is necessary to ensure the trust of the organization's clients as well as its competitive position, while the organization's compliance with its regulatory framework is to be documented.

Due to the increasing dependence of organizations on information and information systems that process them, they face daily increasing business risks due to the emergence of new technological and other threats.

On the basis of these major threats, which are even capable of affecting the sustainability of an organization, it is absolutely necessary to implement measures to minimize these risks. Information security, which manages the part of the business risk that stems from the information systems that are dependent on the organization, is trying to secure this need. A key tool for information security is the establishment of an Information Security Framework, which defines the strategy and all security principles set by the Organization's Management.

Important elements of an Information Security Framework, according to the information security standards, are the information security Risk Assessment Methodology, the Vulnerability Tracking Policy and the Penetration Tests that were analyzed above in the study. Risk Assessment Methodology enables an

organization to recognize and evaluate the risks involved in the security of its information resources in order to organize as much as possible the steps necessary to protect it, as suggested, for example, by OWASP [3].

Alongside the Vulnerability Tracking Policy and conducting security controls, the organization is allowed to maintain an adequate level of security.

Finally, by conducting Penetration Tests, which are one of the tools of a policy of identifying weaknesses and conducting audits, it is possible to identify weaknesses in applications and the infrastructures in which they will operate. As has been extensively analyzed in the study, based on OWASP's proposals [4], penetration testing is not the only security testing tool but is part of a larger design whose size depends on the size of the organization and its information systems, and the data it is required to protect. Also, the implementation of only penetration testing in one application, is not sufficient and it is necessary to control the entire infrastructure.

From the audit report that was conducted, it was found that some of the findings were infrastructure problems and not applications. At the same time, depending on the criticalness of an application or an information system, it is appropriate to develop systems of continuous security monitoring and privacy and security design as proposed by OWASP [5].

Acknowledgements

Authors would like to acknowledge the University of West Attica postgraduate program of studies "MSc in Industrial Automation" for supporting this research project.

References

[1]. OWASP Testing Guide 4 https://www.owasp.org/images/1/19/OTGv4.pdf
[2]. Common Vulnerability Scoring System SIG https://www.first.org/cvss/
[3]. OWASP Testing Guide 4 https://www.owasp.org/images/1/19/OTGv4.pdf
[4]. OWASP Testing Guide 4 https://www.owasp.org/images/1/19/OTGv4.pdf
[5]. OWASP Testing Guide 4 https://www.owasp.org/images/1/19/OTGv4.pdf

D.Kasinas. "Study and Design of Risk Assessment Procedure and Basic Penetration Tests before the Production Environment" International Journal of Engineering Science Invention (IJESI), vol. 07, no. 10, 2018, pp 36-47