universidad de león

Escuela de Ingenierías

Assignment II

Diseño y Programación segura

Alumnos:

González González, Ángel

Máster Universitario en Investigación de Ciberseguridad

Índice

1-Application Security Assessment Questionnaire

This Questionnaire covers the set of security that the ISO offer to member, explains the process for requesting an assessment and provides a questionnaire to understand the target environment. But is not able to assess every possible platform or application.

This questionnaire is divided into 10 steps.

First of all, it gives us the most common assessment scenarios, but can be customized, this assessment should be determined in the first meeting. Some of the assessments this test recommend are:

- Network based
- Host Based
- Application
- Compliance
- Physical Security Assessment
- Enterprise Security Assessment

This are some of the assessments, but you can add others or delete the ones you want.

Then we have the questionnaire that is divided into five questions:

- **Basic Information:** Here you have to put the information about you organization, for example the name, the machines that you have, etc.
- **Audit Information:** In this section, you want to put what do you want in the audit, for example if you want the Information Security Office to perform a host-based assessment, or if you want to perform compliance, physical or enterprise assessment, and some other things you can select.
- **Network Security Information:** Here you have to put some information about the network security of your organization, for example if your organization has ever been compromised, or does your organization use firewalls, or DMZ, and some other questions to cover the network security about your organization.
- **System Information:** In this one, you will put information about the system your organization uses, most of them are about the operative

sistem you are using, for example how many Microsoft professional clients does your organization uses, or other questions like What E-commerce applications your organization uses.

- **Service Information:** This is the las section, and you have to put all the information about the services, for example what type of authentication do you use for your web services, or what antivirus do you use.

ID	The company is Carnegie Mellon ISO
Goal of the questionnaire	This questionnaire is to cover a set of security assessment and assist in understanding the target environment.
Target users	To all the organization that want to improve its security.
Description	The ISO is composed of some points of the process to improve the security, also it has a questionnaire to know the needs of the client.
Positive	You can know how is the security of your organization, and the vulnerabilities it has.
Negative	Is too long and not very specific.

2-Information Security Review Questionnaire - IT Support CUNY

This questionnaire is to identify the information security requirements, and if you use it at the first stages will reduce the risk later.

It is divided into 7 sections that will allow you to know what are the vulnerabilities and the risks, each one is in turn divided into other questions, some of them are square to mark if it meets the question, or questions to be filled writing the answer, these sections are:

1. **Data classification:** Here we want to identify what is the highest sensitivity level of data of the project, for that we have one question that says if the project involves non-public University Information, this is the most important, then we have a subcategories to know better what type of data the project involves, to finalize, we have a question to know why we mark some squares.

2. **Use of vendor IT services:** This section is to evaluate any vendor of IT services and it used to know the security requirements that the vendor will have. It is composed of three questions, two of them are to mark squares and the first question is to know if we will acquire ongoing vendor IT services, if we mark no, we will go to the question three that asks us what service we want to acquire. The second question is to know where we acquire the service.

3. **Identify management, access, control, authorization:** In this section we want to know who has access to the product, that will allow us and determinate if we needs more controls to reduce the risk of unauthorized people, if we want to reconsider what type of users has access at what type of data, or we are already good without any risk.

4. **Network Access and Communication:** This is compose of two questions to mark a square, and another two to write the answer, as this will allow us to know how is the security of the network and the requirements and controls that we are needing.

5. **Data Protection:** Here we will know what type of protections and requirements we already need to protect the data that the project has. With that we are going to reduce to risk of get unauthorized access of people to sensitive information.

6. **Logging and Auditing:** In this section how is the logging activity, and we will know if we are already with a good security, or if we will need another types of features to increase the security and reduce the risks of the log and audit.

7. **Business Continuity:** This is the last section, and it is composed of one question to describe the business continuity and the capability to recover from a disaster, the requirements and provisions that we already have.

ID	The company is IT Support CUNY, the version is the V 1.2
Goal of the questionnaire	This questionnaire is to identify all the risks that the organization has, and to know how the people can access at what type of information, to know if our sensitivity data is protected.
Target users	To all the Universities that want to improve its security and data.
Description	This questionnaire is composed of different sections, with questions of mark different squares, or to write the question, to know how the sensitivity data is protected and what type of people has access to know the risks.
Positive	This questionnaire is divided in several points to specify what typo of risks are you going to cover and has two different type of questions.
Negative	Is too focused in the access of the users has to the sensitive data, but do not see about others risks.

3-Payment Card Industry (PCI) Data Security Standard

This questionnaire is divided into six sections, those sections has a huge type of questions, these questions must be answered by marking a box with yes or no. First of all we have to fill a questionnaire with the information about the business, like the name, a brief description, the providers, etc.

Then appear a Rating Assessment that you have to mark green or red, depending on the most answers of the netx questionnaire.

Now there is a series of sections, specifically 6, in which each section are divided in several requirements, this 6 sections are:

- **Build and Maintain a Secure Network:** Here its cover all relationated with the security of the network.
- **Protect Cardholder Data:** This section is all relationated with the data, to encrypt it and protect it.
- **Maintain a Vulnerability Management Program:** Here its cover the security of programs, like antivirus.
- **Implement Strong Access Control Measures.**
- **Regularly Monitor and Test Networks:** This section includes to monitor and do the necessarily tests of the network.
- **Maintain a policy that addresses information security:** This is the last one and is to cover all relationated with the policy of the company and the information security.

ID	The company is Payment Card Industry (PCI) in the version 1.0
Goal of the questionnaire	This questionnaire is to know if it's secure, or if you have to change anything.
Target users	This questionnaire is for small providers of software
Description	This questionnaire is composed of different sections, with questions to mark different squares with a YES or NO, to know how the security of the company is and if you need to change something.
Positive	It is complete, because it has a lot of sections, and each section has two requirements, which allows it to cover all that is needed.
Negative	It can only be used in scenarios where a credit card is used.

4-Conclusion

In this document has been analyzed three types of questionnaire, I will select the second one to use it in my code, because despite is more focused on University institutions, can be used in my project to see what type of person has access to my system and the data i'm using to do the operations, like the command voices or the coordinates to navigate in the apartment.

5-Questionnaire

1. DATA CLASSIFICATION

Purpose *This section identifies the highest sensitivity level of data that the project involves. This information is needed to determine baseline data security requirements that must be addressed during the project.*

1.1. The project involves: *(check all that apply)*

☐ Non-Public University Information

Subcategories:

☐ Personally Identifiable Information

☐ Educational records and/or other information subject to FERPA regulations

☐ Information regarding an individual's mental or physical condition and/or history of health services use and/or other information subject to HIPAA regulations

☐ Financial information, including credit card and bank information, budgeting, salary and financial aid information

☐ Human Resources information

☐ Research information

☐ Other data the project sponsor considers sensitive, private, confidential or non-public

If any box above is checked, explain the nature, type and quantity of the data and why the involvement of this non-public university data is essential to the system or service to be delivered by the project:

Click here to enter text.

2. USE OF VENDOR IT SERVICES

Purpose *This section describes the intent, if any, to acquire ongoing vendor IT services (e.g., application software hosting, hardware/software infrastructure, data storage facilities, staffing, etc.) in support of this project or service. This information is needed to determine security requirements that should considered when evaluating vendor services and negotiating vendor contracts.*

2.1 Will the project acquire ongoing vendor IT services (e.g., application software hosting, hardware/software infrastructure, data storage facilities, staffing, etc)?

☐ Yes

☒ No. If checked, skip to Section 3.

2.2 The vendor service(s) will be acquired via:

☐ Request For Proposal

☐ Sole Source Procurement

☐ Purchase Order

☐ Agreement to vendor's online license user agreement

☐ Other. If checked, describe here:

Click here to enter text.

2.3 Briefly describe below the service(s) to be acquired, including names of desired vendor(s) if known:

Click here to enter text.

3. Identity Management, Access Control, Authorization

Purpose

This section identifies the user population who will have access to the IT product or service to be delivered by the project, as well as planned security access controls. This information will help determine if additional controls are needed to reduce the risk of unauthorized or otherwise inappropriate access to sensitive data.

3.1. Who will access this application or system?

☒ Faculty

☒ Staff

☒ Students

☐ Consultants and temporary employees

☐ Other (please explain):

Click here to enter text.

3.2. If not covered above, what entities external to the University will have access to the application or service? Click here to enter text.

3.3. Is access limited to only those individuals whose job or function requires such access? Click here to enter text.

3.4. Is any part of the system open to the public or to an anonymous class of users?

All the project is open to the public, it is an open source project.

3.5. Briefly describe the process by which authorization of users will likely be accomplished, if known.

None, the code is uploaded in GitHub and public, they can access it if they want

3.6. Are there different levels of authorization in the system? (e.g., full access, limited access, read-only access, etc.)

All is full access

3.7. Is there an identified authority that approves requests for access to this system? Who would that be?

No

3.8. Is there a process for the access administrator to be notified when a user's status or role changes?

No

3.9. Will there be uniquely identifiable accounts for all users requiring access?

No

3.10. How will accounts which are no longer needed be recognized and deleted in timely and manageable manner?

There aren't any accounts.

3.11. How will this system authenticate users?

☐ CUNY Portal LDAP Single-Sign On

☐ Active Directory (cuny.adlan)

☐ CUNY Enterprise Active Directory

☐ CUNYfirst Single-Sign On

☐ Local Authentication

☐ Other:

Click here to enter text.

3.12. Where local authentication is used, provide details on the enforced password complexity and expiration policy.

There is any authentication.

3.13. Where local authentication is used, provide details on how passwords are securely stored within the system (e.g., encrypted using a salted hash).

3.14. Does the application automatically log off, lock or terminate a session after a predetermined time of inactivity?

There isn't any log off or disconnection, because there isn't any account, isn't needed.

4. Network Access and Communication

Purpose

This section identifies the scope of network access requirements. This information will help determine controls needed to reduce the risk of unauthorized or otherwise inappropriate access to sensitive data.

4.1. Is this system required to be network accessible? ☒yes ☐ no

4.2. If so, will it be accessible:

☐ only within CUNY Central Office networks

☐ only within one or more CUNY Campus networks (specify)

☐ both CUNY Central Office and CUNY Campus networks

☒ the Internet at large

☐ other – please explain:

Click here to enter text.

4.4. Will this system be accessible through means other than the network (e.g., telephone)?

It is only accessible via computer and need the network to function properly.

5. Data Protection

Purpose

This section identifies available data protections and requirements. This information will help determine controls needed to reduce the risk of unauthorized or otherwise inappropriate access to sensitive data.

5.1. Are there restrictions on what quantity or type of data can leave the system?

The data that is used is a real data information, and isn't any restriction of the quantity of data leave the system, because all the data is used in real time, and delete it when is used.

5.2. Are shadow copies of any of the data anticipated to be created? For example, would users copy or download data to their own devices?

The only data that is saved is the coordinated of the apartment, but the users can't upload any data, only interact with the project with the voice.

5.3. Does data associated with this application or system interface with other applications or systems?

No

5.4. Is non-public university data encrypted while at rest?

No

5.5. Is the data encrypted while transmitted over an untrusted network? Click here to enter text.

No

5.6. What type of encryption is used? How is it configured and deployed?

There isn't any encryption.

6. Logging and Auditing

Purpose

This section identifies available activity logging and auditing capability. This information will help determine whether additional logging and auditing features needs to be established.

6.1. Describe logs and/or audit trails that are produced by the application or service.

The only logs that the program has is the real tiem logs, that appear in the command prompt about the command recognised and the navigation.

6.2. Is sensitive data embedded in the logs?

No

6.3. Can logs and/or audit trails link actions to individual users?

No

6.4. Are successful/unsuccessful accesses logged? With client network address?

No

6.5. For how long are logs retained?

When the system ends, the logs are cleaned.

7. Business Continuity / Disaster Recovery

Purpose

This section identifies business continuity and disaster recovery provisions and requirements.

7.1. Is there a documented business continuity / disaster recovery plan that addresses procedures to restore any lost data or functionality in the event of an emergency or other occurrence, the staff responsible for carrying out data restoration, emergency contact names and numbers, important business partners and other business supply information necessary for a temporary office setup to support data restoration?

No.