

Information Security for Managers		
Third party / vendor security		
Unit no: (7)		
Unit (Module) name: Third party / vendor security		
<i>Learning Activities</i>	Streaming Webinar, Text, Self-assessment Exercises, Exercises with answers on discussion forums and within the organized sessions with trainer/mentor, e-portfolios	
<i>Learning Responsible</i>	Gabriel Vladut Valentin Istratie	
<i>Learning Activity Goals</i>	• Risks in Social Networks • Measures to have Security and Privacy in Social Networks • Security techniques • Procurement requirements	
<i>Skills to be Gained</i>	• TS3 Network Security • TS4 Penetration (exploitable vulnerabilities) testing • SS3 Cognitive and behaviour analysis	
<i>Duration of Learning activity</i>	2 weeks	
<i>Learning requirements</i>	What is needed?	
	• Learning about Procurement requirements • Learning about Risks in Social Networks • Measures to have Security and Privacy in Social Networks • Security techniques in Social Networks	

Brief information about the module

Description
Procurement requirements refer to the goods and services that must be acquired from organizations outside the performing organization. For a variety of reasons, sometimes performing organizations rely on vendors to provide what's needed to complete a project. For example, consider the widget manufacturer that undertakes a project to automate their inventory tracking system. Some of the project work activities involve the relocation of storage bins in their main warehouse. Some of the work activities involve custom software development. As to the software development activities, widget manufacturer doesn't have a human resource who knows how to develop the software application. Regarding the software development activities, widget manufacturer must procure those services. Web-based social networks (WBSNs) are online communities that allow users to publish resources (e.g., personal data, annotations, blogs) and to establish relationships, possibly of a different type for purposes that may concern business, entertainment, religion, dating, and so forth. In the last few years, the usage and diffusion of WBSNs has been increasing, with about 300 Web sites collecting the information of more than 400 million registered users. As a result, the "net model" is today used more and more to communicate, share information, make decisions, and 'do business' by companies and organizations. It is then a challenging issue to devise security mechanisms for social networks, able to protect private information and regulate access to shared resources. In this article, besides providing an overview of the characteristics of the WBSN environment and its protection requirements, we illustrate the current approaches and future trends to social network security, with particular attention paid to the emerging technologies related to the so-called Web 2.0. The learners could be informed about such aspects by reading the corresponding text, watching streaming webinars and solving exercises at own pace. All these documents are on the digital interactive project platform. The learners can test their answers on Self-assessment exercises. The answers on other exercises should be saved on the corresponding discussion forum and discuss with the mentor at the common organised meeting once a week. Learner can work cooperatively with other ones and mentor particularly during the meetings. They will be supported to develop e-portfolio important for reflection and evaluation of the training.

Content of the Learning Material

Procurement requirements refer to the goods and services that must be acquired from organizations outside the performing organization. For a variety of reasons, sometimes performing organizations rely on vendors to provide what's needed to complete a project. Procurement requirements refer to the goods and services that must be acquired from organizations outside the performing organization. For a variety of reasons, sometimes performing organizations rely on vendors to provide what's needed to complete a project.
--

The first step in the public procurement process is to identify requirements. All procurement requirements begin with the perception of a need. The need to cross a body of water could create a requirement to build a bridge, a ferry, or other transportation systems.

At this stage it is necessary to clearly define the need, and this may be done by way of a study to determine the best mode to cross the body of water (given the present situation and forecasted future need), then the type of bridge to be constructed, or a comparative cost/benefit analysis to determine the best solution between a bridge and other alternatives.

The study should include if the need can be satisfied in-house or contracted out, quantification of the initial budgetary estimate, and an idea of the procurement lead-time.

Usually, a social network is defined as a small-world network, consisting of a set of individuals (persons, groups, organizations) connected by personal, work, or trust relationships. Social networking is then a quite broad and generic notion, which in the Web context might be applied to any kind of virtual community. For instance, users registered to a Web service, such as Web mail, online journals, or newspapers requiring a subscription, can be considered as a social network. In the following, we adopt the definition, according to which an online community's Web site can be considered a Web-based social network only if it satisfies the following conditions:

- Relationships are explicitly specified by its members, and not inferred from existing interactions (e.g., a mailing list can be used to infer implicit relationships).
- Relationships are stored and managed by using technologies, such as database management systems, allowing relationship analysis and regulating access and retrieval of relationship data.
- Members are able to access relationship information, at least partially.

Key Terms

Relationship-Based Access Control: An access control paradigm specifically tailored to social networks, according to which social network members authorized to access a given resource are denoted in terms of the relationships they must participate in to get the access.

Social Network: A small-world network consisting of a set of individuals (persons, groups, organization) connected by personal, work, or trust relationships. Usually modeled as a graph, where nodes correspond to social network members, whereas edges denote the relationships existing between them.

Privacy-Aware Access Control: In the context of social networks, denotes an access control paradigm where access control requirements of social network members are enforced without disclosing private information about the relationships they participate in.

Web-Based Social Network: A Web-based system that allows its registered members to establish relationships with other members and to share different types of information (e.g., personal data, contacts, multimedia resources).

Social Network Analysis: A discipline aimed at collecting statistical data from the analysis of social network topology.

Relationship Trust Level: In a social network, denotes the value associated with a trust relationship, providing a measure of how much a given member considers another member trustworthy. Depending on the purpose for which it is used, this notion may have different meanings. For instance, in a collaborative rating environment, it denotes how much a given member trusts the opinions of another member with respect to a specific topic (topical trust) or in general (absolute trust). By contrast, in an access control context, it has some similarities to the notion of security

level used in mandatory access control models.

Edge Perturbation: Graph anonymization technique aimed at hiding the actual social network relationships by performing a set of random edge deletions/insertions in the network graph.

Social Network Relationship: A relationship concerning two members of a social network. In WBSNs, besides personal/work relationships (e.g., friend/colleague), also trust relationships may be supported which denote how much a one member trusts another. In the graph representation of a social network, relationships are usually denoted by edges, labeled with a relationship type and/or a relationship trust level.

Graph Anonymization: Technique aimed at hiding private information about social network members when performing social network analysis. Node anonymization and edge perturbation are the two main graph anonymization techniques currently used.

Node Anonymization: Graph anonymization technique aimed at hiding social network members' identities by labeling the corresponding nodes with random identifiers (naïve anonymization), or, in case nodes are associated with attributes which can be used to identify the corresponding user, by using techniques based on k-anonymity (Sweeney, 2002).

Social networks

Communicating and sharing information with those around us is a part of everyone's life and has evolved from simple text messages, to emails and to what we now call social media platforms.

What is not very well known or realized is the fact that our exposure in the online environment comes with a lot of risks.

Social media and social networking or messaging applications can pose a number of security and privacy risks to both organizations and individuals when used in an inappropriate or unsafe manner.

The most popular and widespread platforms on social networks:

- Facebook with over 1,300,000,000 members;
- Flickr used to store, organize and share media files;
- LinkedIn with over 300 million users;
- Instagram with over 30 million users;
- Twitter with over a billion members;
- YouTube with over a billion users;
- Tinder with about 12 million users;
- TikTok with over 800 million users.

Risks

Geotagging

- Represents the addition of geo-identifying data to photos, videos, websites and text messages by applications that can read your location or are allowed to do so in your settings;
- Be sure to turn off geotagging features in sensitive locations to avoid revealing your exact location, where you work, or where you live.

"Audience"

- It's a general term that refers to who is able to see and/or comment on your posts;
- Your friend group can change at any time and be able to view a post that contains information about you. You may intentionally share something with your "friends", but what

they do with the post is beyond your personal control.

Identity

- Describes the range of information that specifically relates to an individual;
- It should be kept in mind that there are people who use social media as a research method to search for identity information, with possible malicious intent, such as identity theft, fraud, embezzlement or intimidation.

Measures

Password

- It is recommended to use a different password for each online account;
- It should be at least 10 characters long and contain uppercase letters, lowercase letters, numbers and special characters;
- It must not be disclosed to anyone, no matter how close or trusted the person we want to tell is;10
- It is recommended not to use personal information when creating a password (eg: parents' names, date of birth, pet's name, etc.);
- Change your password periodically;
- Sign out of your account when you're using a device that's not yours or is being used by someone else.

Do your security updates on time!

- Social media platforms regularly introduce new privacy and security settings. These can be found in your account settings and it is recommended that you check them regularly;
- Use the two-factor authentication (2FA) option to make sure someone isn't trying to hack your account.

Do not accept friend requests from anyone!

- Accept or send friend requests only from/to people you meet in real life or to public people you are interested in by taking care to follow their official profiles;
- DO NOT FORGET! If you feel attached to certain accounts you can restrict their access to your posts or you can block the account. You also have the option to report accounts or posts for reasons such as: fake account, fake name, posts with inappropriate content, incitement to violence, false information, etc.
- DO NOT click!
- Many attackers use social engineering to gain a person's trust in order to later gain access to information;
- Do not open links and attachments from social media if you are not 100% sure of the source (eg websites offering prizes are often intended to steal information);
- If from the chats, a friend seems to be behaving differently (asks a lot of questions, becomes very curious about his personal life, asks for money) there is a possibility that his account has been hacked and an attacker is using it for malicious purposes.

Think twice before posting!

- Social media offers as much an opportunity to create a positive online reputation as a negative one, in addition, even if we "delete" a post, once it has appeared online it cannot be permanently deleted;
- Don't reveal too many personal details on social media! "About Me" fields are optional.

- The boundary between professional and personal life in the online environment
- Do not disclose information about your employer online
- Don't post work photos or negative messages that put the employer in a bad light.
- Think before you post and don't risk your job.

Close old accounts!

- If you have old accounts on social media platforms that you no longer use, or even old accounts on the same platform, try to close them. In this way you create as few links as possible with current accounts being more protected from possible attackers;
- Older accounts or platforms may not be as secure as today's.

Social media poses great risks

- Social networks pose high security and privacy risks due to their centralized architecture, their huge store of personally identifiable information that any hacker would love to have, and the general ignorance of the population about how to properly use social media. privacy settings to improve their online safety.
- Another very high risk, especially among teenagers, is trusting other people and the type of personal information disclosed online.
- This can be combated through technological means and the enforcement of security policies.
- We should consider information transmitted through social media to be insecure and therefore not transmit sensitive information through social media, thus the primary responsibility to stay safe rests with the USER

Bad social media habits

- Social networks are widely used platforms by users today. We have a wide range of possibilities available.
- Some are more geared towards uploading photos or videos, others towards our opinion and in other cases simply to keep in touch with friends and family. In any case, we are dealing with platforms that have many users around the world.
- This also makes hackers set their sights here. We will talk about these habits that should be changed in social networks if we want to keep our privacy and security.
- There are many types of platforms that we can find on the network that give us the opportunity to send messages to friends or family, commenting on photos, videos ...
- This makes them a very popular environment for both private users and businesses.
- However, this also causes you to have some risk to our security and privacy. Hackers can watch here to carry out their attacks. They can especially take advantage of bad user habits when using these platforms.

Habits that need to be changed

- Privacy and security are very important factors for users.
- However, they are not always present.
- We can be victims of many types of attacks that compromise these two factors.
- We can also make mistakes when using social media and it affects us.

Add any type of contact

- A very common error in social networks is adding any type of contact. This can happen on platforms like Facebook.
- It is possible that what we are adding is a bot rather than a real user.

- You need to know how to differentiate them and avoid adding any type of contact that your invite receives.
- Sometimes bots are designed solely to collect user data. This may compromise our privacy. We need to have a real filter on the contacts we add.
- It is important that we have people among our friends who are not a problem for our security and privacy.

Don't connect with social networks from anywhere

- You often log in through social networks on any site. This is very comfortable, but not the best for privacy.
- Certainly on many occasions we find the possibility to register on a page or to connect to a platform through Facebook or Twitter. We avoid registering on that site and filling out a long form. The problem is that we provide personal data to that website through Facebook. This data / information we share can be used by third parties for advertising purposes.

Provide more information than necessary

- It is definitely one of the worst habits that many users have. They enter a lot of personal data, information that is not really necessary, into social networks.
- For example, data such as our phone number, email address, information about where we live ... All this affects our advertising and could be used for bad purposes.
- Don't give more information than is really necessary. In this way we will improve our privacy in the network and we can even avoid certain security problems.

Spreading fake news

- The problem of fake news is still present today. I can reach them through many means, but without a doubt in social networks they are more than presences.
- As we know, it is fake news that they use as bait and can sometimes even distribute malware.
- It is important to avoid sharing this type of fake news and also to access it when we see it on social media.
- This will improve our security.

We do not protect our privacy

- A final mistake is not properly protecting privacy. For example, we leave our profiles open for anyone to enter.
- We provide information to anyone who might collect it to create a profile for us and even send targeted advertising or perform various attacks that affect our security.

Social engineering from an interdisciplinary perspective

Due to the technique used by hackers, it is necessary to approach an interdisciplinary perspective such as information technology, psychology, business and ethics.

The discipline of information technology

- Social engineering should be discussed in the context of current information systems and their defense used as a form of risk mitigation.
- Multi-factor authentication is a common and often effective way for organizations to confirm that the person accessing systems should actually have that access
- An additional factor could be the use of a virtual private network (VPN), i.e. authentication to further validate the user.

Psychology discipline

- It is necessary to understand the concept and understand the thoughts and behaviors of both the attacker and the victim.
- The methods are important for social engineering because they are used to bypass protections that may be in place, such as firewalls and systems used to identify intruders.
- It helps to understand employee actions that are one of the main causes of data breaches.

Business perspective

- it is important because social engineering can affect many types of businesses and have implications for how organizations are structured and managed.
- it helps determine the factors that influence social engineering attacks and is beneficial if considered in more specific terms in relation to the following business areas: training and development, documented policies, internal audit procedures, budgets and organizational culture.
- can detect deficiencies in any of the areas that may contribute to attacks.

Ethical perspective

- it is important in the context of social engineering and related research because the idea of manipulating another human being violates many ethical principles.
- helps, in the case of a social engineering event, to treat the victims.

It is important to consider:

- each discipline, providing information on how to understand and interpret the subject, protect against different types of attacks, and understand the impact of social engineering from both a human and organizational perspective.
- that each discipline's interpretation of the subject is useful only when viewed in the context of the other disciplines.

Security techniques

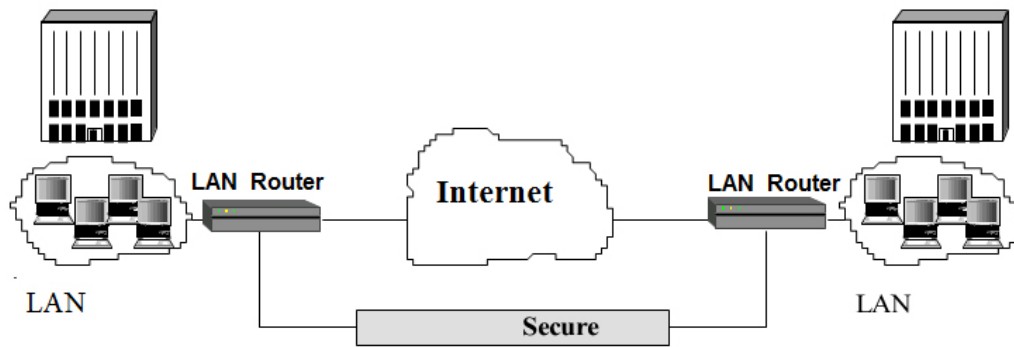
- Equipment inventory
- Inventory of applications and operating systems
- Wireless equipment control
- Network security design
- Limiting and controlling network ports, communication protocols and services
- Protection of perimeter areas
- Physical access to locations
- Controlled use of administrative privileges
- Monitoring and controlling user accounts
- Skills assessment and security training

Security techniques**VPN (Virtual Private Network)**

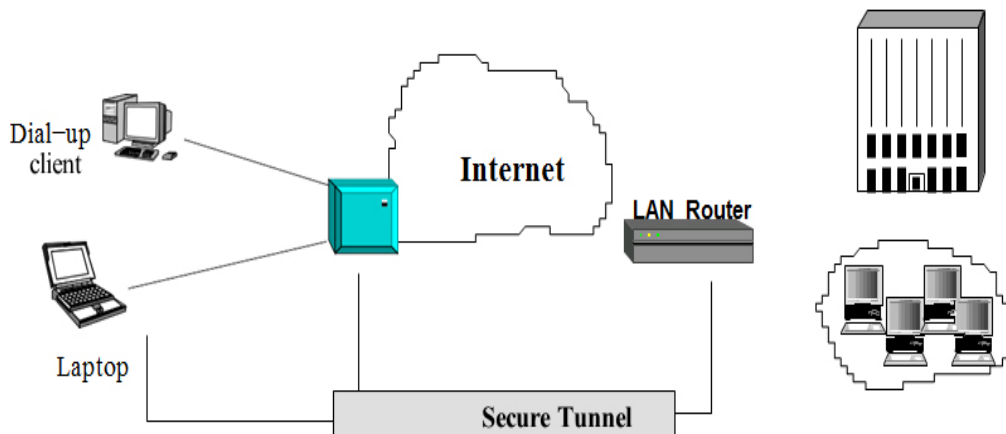
A virtual private network is a secure connection over an insecure network such as the Internet. Virtual means the existence of a unique network, regardless of topology, that is, a group of geographically distributed computers that communicate and can be administered as a single network.

Private means a virtual network with access control. which provides confidentiality, the integrity of messages and authenticates between the users and the computers participating in the

communication.

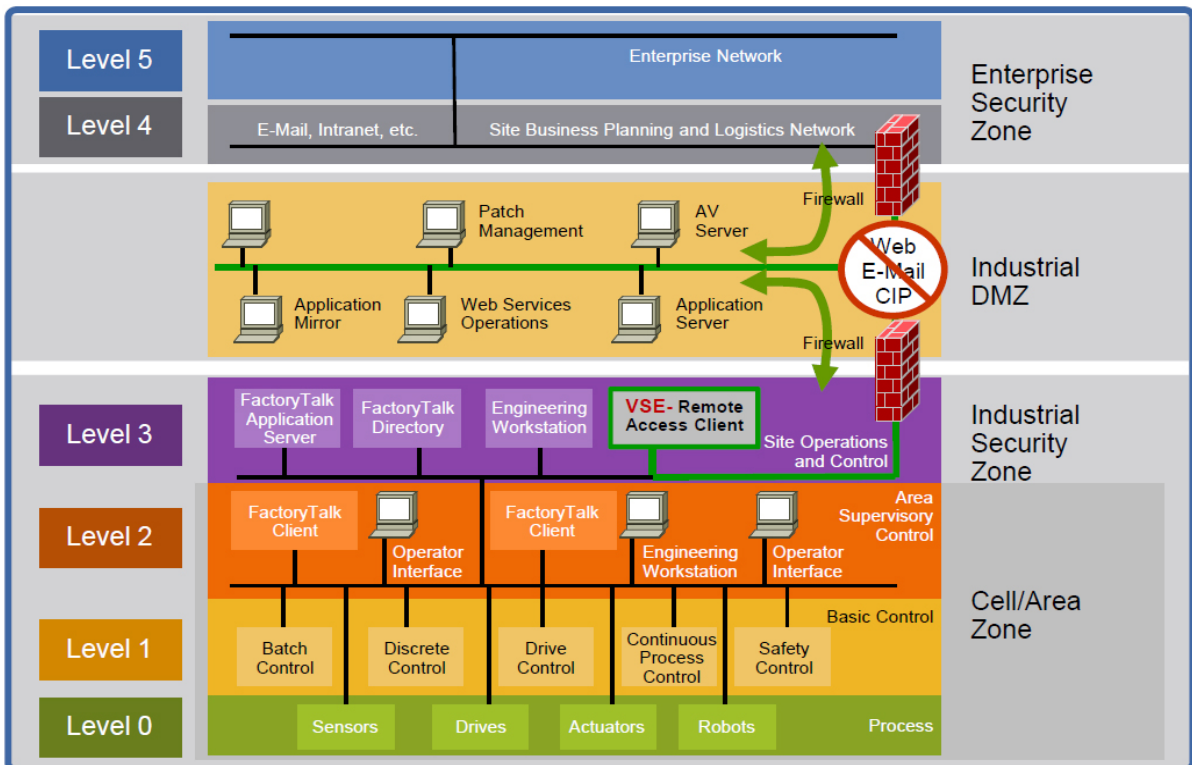


VPN (Virtual Private Network)



VPN for remote access

Creating a secure industrial infrastructure



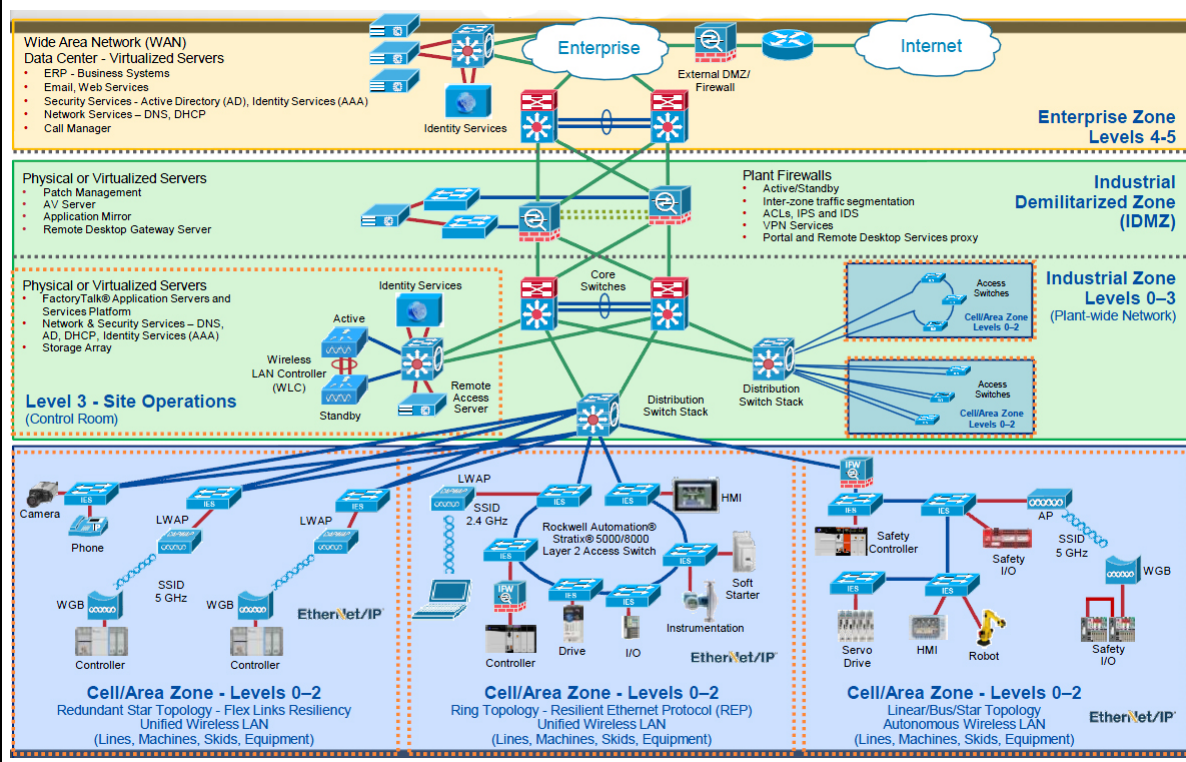
ISA 95 Logic Model - Industrial Automation and Control System (IACS)

- Defense-in-Depth (DiD) supports this approach. Based on the notion that a single point of protection can and likely will be defeated, DiD security establishes multiple layers of protection through a combination of physical, electronic and procedural safeguards.
- A bank uses multiple security measures—such as video cameras, a guard, and a vault—this helps ensure that threats meet more than one line of defense.
- A security-in-depth approach comprises six main components:
 1. Policies and Procedures
 2. Physical
 3. Network
 4. Computer
 5. Application
 6. The device

Creating a secure industrial infrastructure

- Physical security should limit personnel access not only to areas of a facility, but also to entry points into the physical network infrastructure, such as control panels, cabling, and devices.
- Segmenting plant areas into virtual local area networks (VLANs) is a network-wide security best practice.
- Smaller VLANs are easier to manage and maintain in real-time communications.
- They can help isolate devices from those that have been compromised, which keeps the negative impact within a single VLAN.
- One of the technologies discussed should be an industrial demilitarized zone (IDMZ), which creates a critical protective barrier between the enterprise and industrial areas.
- An IDMZ restricts traffic from traveling directly between the two zones and can help better manage access by enforcing authentication or monitoring traffic for known threats.

Creating a secure industrial infrastructure



Questions:

Questions Discussion Forum to be answered with a short explanation. Answers will be discussed with the mentor during the mentoring sessions

1. Which are the Risks in Social Networks
2. Measures to have Security and Privacy in Social Networks
3. Which are the main Security techniques in Social Networks

Self-assessment questions. After answering the learner can see the results and compare them with these saved on the platform

- Risks in Social Networks
- Security and Privacy in Social Networks
- Security techniques

Attachments (PowerPoint presentation, handouts, prints, links, video...):

References:

Procurement Requirements

URL: [Procurement-requirements](#)

Procurement Requirement Determination

URL: <https://www.procurementclassroom.com/procurement-requirement-determination/>

Security and Privacy in Social Networks

URL: <https://www.igi-global.com/chapter/security-privacy-social-networks/14073>

Security and Privacy in Social Networks

URL: <https://sefcom.asu.edu/publications/security-privacy-social-ic2011.pdf>

Privacy and Security in online social media

URL: <https://www.geeksforgeeks.org/privacy-and-security-in-online-social-media/>

Data Security Techniques and Privacy

URL: <https://www.educba.com/data-security-techniques/>

What is Security Techniques

URL: [Security-concepts-developments-and-future-trends](#)

Most Effective Security Techniques

URL: <https://dzone.com/articles/most-effective-security-techniques-part-1>