CIS-481: Introduction to Information Security

InfoSec Chapter Exercise #5 - Option B

Team: Project Team 11
Participants: Sohal Patel, Erika Maglasang, Nathan Moran, Gabriel Rolink, and Tyler Samuelson

Logistics

A. Get together with other students on your assigned team in person and virtually.
B. Review the two options available and decide on only one to pursue as a team.
C. Discuss and complete this assignment in a collaborative manner. Don't just assign different problems to each teammate as that defeats the purpose of team-based learning.
D. Choose a scribe to prepare a final document to submit via Blackboard for grading, changing the file name provided to denote the number of your assigned **Team**.

Problem 1
Review the article linked below:

Transitioning from DIACAP to RMF

Department of Defense (DoD) information systems must be protected with adequate, or acceptable, security controls. As we learned in Chapter 1, if too few controls are implemented, a system is left highly vulnerable to attack. But if too many controls are put in place, valuable resources are wasted with no tangible benefits. This leaves system owners with several challenges:

- What is the process for defining "adequate" security for each system?
- How many controls should be utilized and specifically what should they be?
- Is there a standard list of controls to choose from?
- Who, within the organization, is ultimately accountable for any breaches in the system?

The challenges above were the driving factors behind the development of the DoD's first Certification & Accreditation (C&A) process and all its subsequent revisions from DITSCAP (Defense Information Technology Security Certification and Accreditation Process) to DIACAP (Defense Information Assurance Certification & Accreditation Process), and now RMF (Risk Management Framework).

a) From the DIACAP standard Certification and Accreditation Process Handbook for Certifiers, define: *(5 points each)*
   i. Certification
   ii. Accreditation
b) Describe the DoD system certification and accreditation processes, highlighting the three most important improvements in the transition from DIACAP to RMF, in your view. *(40 points)*

- **What is the process for defining "adequate" security for each system?**

If the proper controls are set in place the security will be enhanced immensely, but the daily tasks of an organization will experience an influx of daily activity. An adequate security can be defined as follows. The main purpose of DoD is to focus on three core tasks: confidentiality, integrity and availability of organization's sensitive information and to save it from phishing (stealing of data). An organization who wants to adequately supply security wants their data secure, but also easily accessible for employees that need to access in daily. Normalized security can be implemented into the organization by including personalized data security controls. These controls should be set up in a way that allows access to individuals who have high authority in the company. All systems can be secured if this method is used, but it may differ depending on the type of organization.

- **How many controls should be utilized and specifically what should they be?**

The controls should be dependent on the Nature of Organization. If high security controls are what the organization desires, the organization should use a cyber security model that complies with the DoD (Department of Defense) U.S. Govt. Anything that falls within the ISO FAMILY; 27000, 27001, 27031, 27032 is also acceptable. All of these laws provide high security controls. GDPR also provides data security controls. All security regulations should be used so that the organization is well protected from cyber-attacks. Otherwise, dynamic strategies should be implemented for high authorities of organization.

- **Is there a standard list of controls to choose from?**

Yes, according to our perspective we would make a list of laws that should be used to protect the data security of the organization.

  - CMMC – an initiative of D.o.D
  - D.F.A.R.S also an initiative of D.o.D
  - The N.I.S.T C.S.F is an intentional structure basically proposed for basic foundation associations to oversee and moderate digital security chance dependent on existing best practice.
  - ISO Family
  - GDPR LAWS AND REGULATIONS

- **Who, within the organization, is ultimately accountable for any breaches in the system?**

Social engineering attacks; lead to security breaches within an organization. Sometimes employees are sent into the organization by hackers, but the most common perpetrators are cyber terrorists. They can cause breaches in security systems from within the organization or social engineering attacks. These attacks can be prevented if employees go through training that will prepare them for potential security breaches. The most detrimental attack to an organization can be theft or leakage of sensitive information of an organization. When that happens the person, who will be held accountable is the person who created the security plan. The plan will be scrutinized for its lack or excess of security controls.

The challenges above were the driving factors behind the development of the DoD's first Certification & Accreditation (C&A) process and all subsequent revisions from DITSCAP (Defense Information Technology Security Certification and Accreditation Process) to DIACAP (Defense Information Assurance Certification & Accreditation Process), and now RMF (Risk Management Framework).

A. From the DIACAP standard Certification and Accreditation Process Handbook for Certifiers, define:

I. **Certification:**

> "When security professionals evaluate a particular system, they actually don't certify anything; they "assess" it and provide recommendations. In DIACAP this recommendation was incorrectly called a "certification", leaving many wondering why they still couldn't go live after their system was "certified". To avoid confusion, RMF will call this step an "assessment"."

A security affirmation implies that an association is following an outsider's legal/ viable set of rules and regulations. This results in better data security. As these organizations are able to provide security to sensitive information within the organization therefore protecting it from hackers.

II. **Accreditation:**

> "The second part of the process is similarly confusing, after "certification" the recommendation was sent to a Designated Accrediting Authority (DAA). The DAA's signature actually completed the "accreditation" portion and allowed the system to go live or remain in operation. But really the DAA's role is to "authorize" the assessment instead of "accredit" it."

Accreditation is the acknowledgment of a person's responsibility for or achievement of something. The work must be acknowledged by the DAA first before the system goes live to the public.

B. Describe the DoD system certification and accreditation processes, highlighting the three most important improvements in the transition from DIACAP to RMF, in your view:

On the off chance that all frameworks are arranged, broken down, made sure about, surveyed and approved utilizing similar rules and guidelines; the framework can then go through the approval process. After it is approved it can be connected to its organization without a tedious and exorbitant re-approval process. The usage of CIA Triad provides privacy for authentication of the sensitive client information, integrity of data, and authorization of data. The availability of data has been enhanced from DIACRAP to RMF in order to provide enhanced security service. Secondly, the security has been improved to a greater extent. Some major improvements are its ability to secure sensitive information for an organization from Data

Phishing and cyber activism. Thirdly, R.M.F has incorporated progressing security exercises, as opposed to desk work concentration. With that in mind, there is a stressed importance on the consistent checking of the security framework for important occasions. The expectation is that the frameworks in the long run will move away from the conventional multiyear life cycle, and persistently progress, observe, and approve of the expulsions of the requirements of years prior.

Work Cited

DIACAP vs. RMF - 10 Major Improvements: TechRoots Blog. (2020, January 21). Retrieved June 13, 2020, from https://phoenixts.com/blog/diacap-vs-rmf/