**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**

1. Get together with other students on your assigned team in person and virtually.
2. Review the two options available and decide on only one to pursue as a team.
3. 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.
4. 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](https://phoenixts.com/blog/diacap-vs-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).

1. From the DIACAP standard [Certification and Accreditation Process Handbook for Certifiers](https://www.hsdl.org/?view&did=440784), define: *(5 points each)*
   1. Certification
   2. Accreditation
2. 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?**

In order to keep adequate security services for all the systems, of DoD for organizations; even though completing the controls lead to enhanced security but the daily task of organization has been hindered badly. The main purpose of DoD is to focus on three core task’s confidentiality, integrity and availability of organization’s sensitive information and to save it from phishing (stealing of data). The organization who want to use adequate system that is they want data security; but flexibility too, so in order to lead to normalized security; the organization should conclude its personalized data security controls and they should be dire confidential only higher authorities of organization should devise method’s ; this would totally depend on how the task adhocracy is and what is the nature of organization

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

The controls should totally depend on the Nature of Organization. In case if organization, wants high security controls so organization should use cyber maturity model compliance it is also an initiative of DoD (Department of Defense) U.S. Govt. Other than that ISO FAMILY; 27000, 27001, 27031, 27032 all of these laws also provide high security controls. GDPR also provides data security controls. In case of following any regulations all of its security controls should be used so that the organization could get save from cyber-attacks. Otherwise, dynamic strategies should be pertained as per the mindset of high authorities of organization.

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

Yes, according to my perspective I’d make a list of law’s whose list should be used to pertain data security of 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?**

The social engineering attacks; lead to form security breaches within an organization and the employees sent in the organization by hackers or cyber terrorists are also a major reason to cause the breaches in the system from within the organization or social engineering attacks which led to psychological training of employees cause the biggest damage to organization by stealing or leaking the sensitive information of an organization.

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).

1. **Certification:** A security affirmation implies that an association is following an outsider's or legal/ viable set of rules and regulations. This results into better data security. As these organizations are liable to provide security to sensitive information of organization from hacking.
2. **Accreditation:** Accreditation along with certification leads to responsibility of an organization to provide enhanced security services