1. According to the publication, how should risk management be undertaken by the organization? Describe the levels involved and how these impacts the overall approach to the RMF?

The decisions related to risk management are usually taken considering

* Mission or business objectives of organization
* Modernization initiatives for systems, components, and services
* Enterprise architecture and the need to manage and reduce the complexity of systems through consolidation, optimization, and standardization
* Allocation of resources to ensure the organization can conduct its missions and business operations effectively, efficiently, and in a cost-effective manner

Level 1: Organization

Level 2: Mission/Business Process

Level 3: Information System

Level 1 and Level 2 activities are Critical as they Preparing the Organization to Execute RMF

risk decision at organization and mission/business process levels guide towards the decision to be taken at information system perspective in Level 3

Multi-Level Approach to Risk Management address the security and privacy risk at organization level, Mission/Business Process Level and information system level. There will be bi directional information flow across 3 levels

**Impact of the level on overall RMF approach:**

The Risk decision taken at level 1 and level 2 impact the selection and implementation of controls at system levels.

Taking enterprise architecture into the consideration Controls are designed by the organization as system specific, hybrid or common. traceability of controls are established by organizations to satisfy security and privacy requirements

Risk management is the holistic approach wherein lot of other aspects of organization are taken into consideration which include mainly mission and business planning activities, enterprise architecture, SDLC process, and system engineering activities.

1. List and describe the steps of the RMF.

The 7 steps in RMF which are essential for successful execution of RMF:

* **Prepare:** The context and priorities for managing security and privacy risk should be established to execute the RMF from Organization Perspective.
* **Categorize:** The system and the information processed, stored and transmitted by the system based on an analysis of **Impact Loss**
* **Select**: Based on the risk assessment an acceptable initial level of the set of controls were set for the system.
* **Implement:** This describes how the controls were set and carried out within the system and its environment of operation
* **Assess**: These controls ensure that the controls which are implemented are in the right place and doing its operation and fetching the desired outcomes with respect to satisfiable privacy and security requirements
* **Authorize** the system or common controls based on a determination that the risk to organizational operations and assets, individuals, other organizations, and the Nation is acceptable.
* **Monitor:** The system and the associated controls on an ongoing basis to include assessing control effectiveness, documenting changes to the system and environment of operation, conducting risk assessments and impact analyses, and reporting the security and privacy posture of the system.

3.) Under the Prepare step, a number of tasks are listed in Appendix E. How are these separated based on levels and who are primarily responsible across those two levels?

The Tasks in the prepare step are divided into 2 levels mainly:

* 1. Organizational Level
  2. System Level

The Primary responsible persons Across Organization Level are senior Agency information security officer or Senior Accountable officials

The Primarily responsible persons across System level are Business Owner or System owner or Authorizing officer

4.) Look across the remaining steps in Appendix E. How is this similar to the discussion in class concerning risk identification?

The Risk terminologies which were discussed can be seen in the steps which are defined or mentioned in the Appendix E. Identifying the Asset which is endangered by the threats and threats lead to vulnerabilities which results in the exposure of the system which is Risk, Risks are mitigated by safeguards of the system which in turn protect the Asset.

Assets identification, Threat detection, Identifying the vulnerabilities and protect the system from exposure and risk management is discussed in large scale with some safeguards which could be applicable to the whole system in the whole organization which protects the Assets.