Infrastructure and Security Risk Management

5.1 – **Technical Infrastructure**

- 5.1.1 - The repository shall identify and manage the risks to its preservation operations and goals associated with system infrastructure.
  - 5.1.1.1 - The repository shall employ technology watches or other technology monitoring notification systems.
    - 5.1.1.1.1 - The repository shall have hardware technologies appropriate to the services it provides to its designated communities.
    - 5.1.1.1.2 - The repository shall have procedures in place to monitor and receive notifications when hardware technology changes are needed.
    - 5.1.1.1.3 - The repository shall have procedures in place to evaluate when changes are needed to current hardware.
    - 5.1.1.1.4 - The repository shall have procedures, commitment and funding to replace hardware when evaluation indicates the need to do so.
    - 5.1.1.1.5 - The repository shall have software technologies appropriate to the services it provides to its designated communities.
    - 5.1.1.1.6 - The repository shall have procedures in place to monitor and receive notifications when software changes are needed.
    - 5.1.1.1.7 - The repository shall have procedures in place to evaluate when changes are needed to current software.
    - 5.1.1.1.8 - The repository shall have procedures, commitment and funding to replace software when evaluation indicates the need to do so.
  - 5.1.1.2 - The repository shall have adequate hardware and software support for backup functionality sufficient for preserving the repository content and tracking repository functions.
  - 5.1.1.3 - The repository shall have effective mechanisms to detect bit corruption or loss.
    - 5.1.1.3.1 - The repository shall record and report to its administration all incidents of data corruption or loss, and steps shall be taken to repair/replace corrupt or lost data.
  - 5.1.1.4 - The repository shall have a process to record and react to the availability of new security updates based on a risk-benefit assessment.
  - 5.1.1.5 - The repository shall have defined processes for storage media and/or hardware change (e.g., refreshing, migration).
  - 5.1.1.6 - The repository shall have procedures in place to monitor and receive notifications when software changes are needed.
    - 5.1.1.6.1 - The repository shall have a documented change management process that identifies changes to critical processes that potentially affect the repository's ability to comply with its mandatory responsibilities.
    - 5.1.1.6.2 - The repository shall have a process for testing and evaluating the effect of changes to the repository's critical processes.
- 5.1.2 - The repository shall manage the number and location of copies of all digital objects.
  - 5.1.2.1 - The repository shall have mechanisms in place to ensure any/multiple copies of digital objects are synchronized.

5.2 – **Security Risk Management**

- 5.2.1 - The repository shall maintain a systematic analysis of security risk factors associated with data, systems, personnel, and physical plant.
- 5.2.2 -The repository shall have implemented controls to adequately address each of the defined security risks.
- 5.2.3 - The repository staff shall have delineated roles, responsibilities, and authorizations related to implementing changes within the system.
- 5.2.4 - The repository shall have suitable written disaster preparedness and recovery plan(s), including at least one off-site backup of all preserved information together with an off-site copy of the recovery plan(s).