# Checklist for Upgrading System Hardware

## Data Classification and Inventorying

- [ ] Assess risks and identify key data.
- [ ] Assign risk categories (low, moderate, high).
- [ ] Clean all mirrors and glass surfaces
- [ ] Create a classification policy outlining data sensitivity levels (public, internal, confidential, restricted).
- [ ] Categorize data by type (documents, databases) and purpose (financial, operational).
- [ ] Identify data locations throughout the organization.
- [ ] Use the categorization policy for data labeling and tagging.
- [ ] Ensure compliance with ISO 27001 Annex A 5.12.

## Data Backup and Verification

- [ ] Develop a comprehensive data backup plan.
- [ ] Define the scope, frequency, format, retention, and roles of data backups.
- [ ] Ensure compliance with ISO 27001, ISO 27002, and ISO 27040.
- [ ] Utilize checksums, hashes, or digital signatures to verify data integrity.

## Perform Data Sanitization

- [ ] Wipe storage devices thoroughly before retirement or sale.
- [ ] Adhere to the organization's media data sanitization policy.
- [ ] Audit records to affirm secure data destruction.
- [ ] Choose reliable data destruction software (e.g., BitRaser).
- [ ] Refer to NIST guidelines or IEEE 2883-2022 for media sanitization best practices.

## Handling of Failed Media Sanitization

- [ ] Isolate and label media with bad sectors.
- [ ] Physically destroy drives with bad sectors as per NIST guidelines.
- [ ] Maintain records of physical destruction.

## Configure New Hardware: Update Software and Install Operating System

- [ ] Retrieve data backup on new hardware.
- [ ] Ensure all software applications are up to date (drivers, antivirus, etc.).
- [ ] Verify software compatibility with new hardware components.
- [ ] Consider reinstalling the operating system for major changes (e.g., new motherboard/CPU).
- [ ] Use migration tools if necessary to transfer OS and software settings.