Introduction:
The state of development of trusted digital repositories is not far from infancy. The Library community in association with their technology partners is just beginning to understand the technical requirements needed to build a trusted repository system. Best practices for implementing trusted digital repositories in a campus environment like Yale are nascent and the road to maturity is likely to be painful and expensive. But beginnings are also an opportunity to perform the right site preparation work so that future development is guided by reasonable models and best practices of the time. The audit checklist (a best practice) for the certification of Trusted Digital Repositories promulgated by RLG (2005) used the OAIS model to define four component of a trusted digital repository system. This best practice focuses upon the Technologies and Technical Infrastructure of a Trusted Digital Repository, specifically the operating system.

Operating System Definition:
Wikipedia defines an operating system as “a special computer program that manages the relationship between application software, the wide variety of hardware that makes up a computer system, and user of the system.” Operating system can be classified as (1) multi-user (2) multiprocessing (3) multitasking (4) multithreading and (5) real time. Modern operating systems like Windows and Linux hide almost all of the complexity of an operating system from an end user.

Role of Operating Systems and Trusted Digital Repositories:
If we view a trusted digital repository as a computational system then its heart is the operating system. Like any software application an operating system is subject to software failure and technological obsolescence. Operating system failures result in the cessation of the core functions of a computing system and the termination of any dependent application like an ingest system for SIPs. Without a running operating system there is no cpu processing, no means to address data in memory or access data on disk storage and network connectivity or communication becomes unavailable. In short an operating system failure is akin to a heart attack in a person. All systems stop until the heart is brought back online. The longer an operating system is unavailable the more likely there is collateral consequences down stream. Internally operating system failures can precipitate disk failures and loss of data held in memory. Externally end user access to the repository is shut down until the operating system and any dependent system i.e. storage is restored. The Library, then serves a community interest by recommending best practices which serve to maintain the reliability and availability of an operating system and to provide strategies to maintain operating systems which are threaten by software obsolescence. In a campus environment where a trusted digital repository system may be composed of smaller federated systems this becomes an important issue.
Maintenance of Operating Systems: Practical Considerations:
Standard system administration procedures should apply to operating system installations and ongoing maintenance to reduce the risk of operating system software failure and obsolescence. At Yale this involves following ITS approved installation and change management procedures and encouraging vendors to make their applications compatible with new versions of an operating system.

Issues to Consider Regarding Operating System Installation and Maintenance:
Scholarly work in a large research institution like Yale spans many academic domains. Trusted repositories that preserve image, text and audio visual collections are likely to represent the typical collection in a library repository. However, special repositories are likely to exist for scientific data that is in a domain specific format. This data is likely to be stored in databases that run on proprietary applications with specialized operating systems. A set of best practices to manage this type of repository could benefit scientists that normally do not focus their attention on preservation of data.

Recommendations and Best Practices for Operating System Integrity in a Trusted Digital Repository:
The operational integrity of a repository operating system is dependent upon its technical and administrative environment. Trusted repositories maintain by the Library or other campus organization should adhere to ITS policies that are used to manage enterprise system. At infrastructure level the repository must have backup and disaster recovery functionality. At the system administration level operating systems should be protected from any single point of failure. This can achieved by following ITS data center procedure for operating system installation and maintenance.