User authentication and security are directly related to access privileges. Authentication includes the methods used to verify that the users are who they say they are. In automated KM systems, authentication based on username and passwords is increasingly supplemented with biometric systems that rely on images of the user's fingerprints or retina. Security involves keeping unauthorized users from accessing, modifying, or destroying valuable information. A related issue is privacy, which is accomplished by maintaining certain information out of the reach of those without access privileges and need to know. In most KM programs, the ability of someone in the organization to modify information once it has been created or added to the system is especially guarded and tracked.

Access time is also a function of the ability to locate specific information in any phase of the KM life cycle, which is directly related to the methodology and vocabulary used to archive, locate, and retrieve information. As detailed in Chapter 5, the methodology and technology used to track the location and version of information in the KM life cycle also affect accessibility.

Intellectual Property

The intellectual property issues associated with each phase of the KM life cycle have legal and practical implications. For example, there is the issue of specific intellectual property rights, such as moral rights, that may allow a knowledge worker to claim authorship of information even if other intellectual property rights have been assigned to the company. There is also the issue of the amount of author involvement in the KM life cycle once the information has been created.With information acquired outside of the corporation, such as stock artwork or work for hire, the issue of ownership verification, the process of verifying intellectual property ownership, arises.