A university operates a centralized information system hosted in a server room that includes a web server, an online learning platform, and an email server. These servers store sensitive data such as personal information of students and staff, usernames and passwords, as well as educational content and student submissions. Some courses are paid and are only accessible after authentication. Users (students, teachers, and administrative staff) can access the services either from the university's local network or remotely via the Internet. The local network connects administrative offices, classrooms (equipped with computers and interactive screens), and the servers, and it is connected to the Internet through a main router. In practice, user accounts are often shared among students, some passwords are weak and rarely changed, and security updates for the servers are not regularly applied in order to avoid service interruptions. In addition, no formal backup policy is clearly defined, and access to different resources is not strictly separated according to user roles. However, the university requires that services remain continuously available (24/7) and that data (especially grades and student submissions) must neither be modified nor accessed by unauthorized individuals.

Follow the steps of risk management to analyze the security of this system.