# Controls, objectives, and procedures in IT audit

Protecting interconnected systems requires controls/safeguards/protections. Controls are designed, deployed, and monitored by control processes. Auditors make sense of things even when they don’t completely understand. This section begins with concepts and paradigms to help you organize your thoughts about how the ERP would be protected and how an auditor might go about assuring stakeholders that risks are understood and addressed.

**Controls** are safeguards put in place to achieve control objectives. But broader control definitions – for example the definition from FISCAM included in an appendix – emphasize that internal control is a process. **Control processes** are ongoing efforts. You need good processes if you want a system of controls that are and will remain effective over time. Auditors validate controls and processes intended to achieve **control objectives**. In general conversations, the term “control” is used ambiguously. But, at the end of the day, internal control audits should focus on whether or not management assertions about how risk is addressed are justified.

Consider this control objective: “*Accounts with administrative or elevated access to shared resources (privileged accounts) are controlled and monitored to ensure they are used only for authorized activities.*” One or more processes manage ‘privileged’ accounts. Roles that require such access are identified, requests for access are reviewed and approved, user directory settings are adjusted, appropriate policies for passwords and multi-factor authentication are created and enforced, usage is recorded and monitored, and – importantly – the whole mix of activities should be reviewed to make sure it remains effective.

Some elements are tangible. Multi-factor authentication tools are installed and configured. Logs of activity (especially privileged account activity) are collected, protected, and monitored. Password rules are configured. And some activities that seem “process like” are also considered controls. For example, there need to be procedures to be sure that when an employee with privileged access leaves, their access rights are suspended. Tangible things are directly observable. Process things often need documentation. For example, you can look to see who is able to make configuration changes by inspecting system settings, but if management approval of a new authorization is to be auditable, the approval might need to be documented in a ticket or memo.

IT audit objectives are often closely related to control objectives. If management implicitly or explicitly asserts that privileged access is appropriately managed, monitored, and secured an auditor maybe be charged with providing assurance of this assertion in an objective such as: “Determine whether privileged access is appropriately managed, monitored, and secured.” Building on some authoritative guidance about how such accounts should be managed, the auditor would then develop a set of procedures that inspect, test, confirm, trace, recompute, inquire, vouch, or compare available evidence in light of expected practices. These procedures employ well-justified criteria. These criteria are generally derived from authoritative sources such as organization policy or standards published by government, semi-government, or industry authorities.

As you work on this case, the goal is to apply concepts from the heart of IT auditing. For the BigU ERP system, privileged access management is of vital concern. But it is only one of many control processes of interest. Networks, applications, devices, data centers, and users are protected by a wide variety of controls and control processes. As you think about the material, try to identify control objectives and think about what it takes to accomplish them. Along the way, you will build skills to formulate audit objectives, procedures, and criteria to collect evidence related to management assertions and thereby fulfill the assurance purpose of an IT audit.

The concepts here are further explored and mastery is evaluated in an exercise. Hopefully students will observe that this discussion applies concepts covered in other course materials.