**Compliance Within the User Domain**

* **Preventive controls**—Mechanisms called preventive controls, such as locked doors or computer access controls, keep an undesired action from happening.
* **Detective controls**—Mechanisms called detective controls, such as motion detectors or usage log analysis tools, recognize when an undesired action has occurred.
* **Corrective controls**—Mechanisms called corrective controls, such as the procedure to remove viruses or a firewall to block an attacking system, repair damage caused by an undesired action and limit further damage.

**Business drivers** are the components, including people,information, and conditions, that support business objectives. Any negative impact on

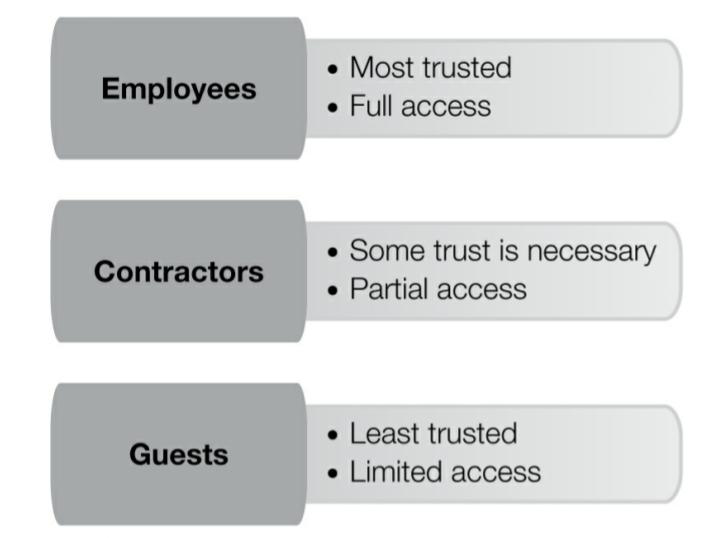
business drivers can also have a negative impact on your organization’s ability to satisfy

business objectives. Carefully research the impact on business drivers before you implement any compliance controls.

In the User Domain, an acceptable use policy (AUP) for each type of user serves

as a training guide and direction document for other controls. Simply put, the AUP is a statement of which actions are acceptable and which ones are not.

**Items Commonly Found in the User Domain :**

****

The following are different types of documentation in the User Domain that

affect compliance:

• **Human resources (HR) manuals**—

**• IT asset AUPs**

**•** **Internet AUPs**—Internet AUPs define proper and improper use of an organization’s

Internet access.

• **E-mail AUPs**—E-mail AUPs define proper and improper use of an organization’s e-mail

capability.

Separation of Duties

The concept of separation of duties requires that users from at least two distinct roles be

required to accomplish any business-critical task. This means that users from at least two roles must collude to compromise data security. Although collusion is still possible, it is far less likely than if a single user could gain exclusive access to sensitive data without anyone else looking. Going further, separation of duties helps avoid conflicts of interest. For example, the role in charge of administering a system should not be the same role that audits that system for potential compliance violations.

Least Privilege:

The first step in implementing separation of duties is to remove unnecessary user privileges.

Any unnecessary privilege provides an opportunity for a user to violate the AUP and perform unauthorized data access. It makes sense to use access controls to prevent unauthorized.

* Confidentiality and NDA Agreements
* Employee Background Checks
* Acknowledgment of Responsibilities and Accountabilities
* Security Awareness and Training for New Employees