Recommendations by Control Classification

1

Establish and maintain an inventory

- Users are expected to follow standards for managing computers connected to the network and have registered network addresses.
- The OS and owner should be included along with the data provided.

2

Recognize the importance of passwords

- Users must use only strong passwords. The IT department should provide password guidance.
- Create departmental accounts for work groups to prevent/avoid password sharing.

3

Make patching automatic

- Each machine should be configured to patch automatically for OS and basic software patching.
- Set up a process that works for the department and helps to minimize disruptions at inconvenient times.
- Automate workstations to enable system administrators the time to give servers the attention required to minimize the impact on services offered.

4

Allow easy recovery with backups

- Helps with user mistakes and hardware failure.
- Backups should be made offsite for increased security.

5

Eliminate many vulnerabilities with proper system administration

- System compromises can be time-consuming and damage credibility and the business integrity.
- Information from enterprisewide scans helps to identify vulnerabilities on each system and provide a baseline for comparison when system integrity is in question.

6

Install antivirus software with automatic updating

- Antivirus software with an automatic DAT file should be updated at regular intervals, for example: no less than weekly.

7

Eliminate unnecessary services

- To improve basic security and minimize effort to maintain systems, workstations should offer only needed services.
- Many OSs are installed with services turned on.
- By removing services, the chance that a workstation will be compromised is reduced and security risk is minimized.

Source: *IT Audit Fundamentals Study Guide*, Figure 2.2 Control Classification

©2022 ISACA. All rights reserved.

ISACA