Primary ITGC audit controls

1.0 Physical and environmental security

- [ ] 1.1 Secure entrances to technology areas using proximity cards, motion detectors, biometric scanning and closed-circuit television cameras.
- [ ] 1.2 Put HVAC systems in place and maintain them on a regular basis.
- [ ] 1.3 Regularly test fire detection and suppression systems.

2.0 Logical security

- [ ] 2.1 Use two-factor authentication to protect access to systems and data.
- [ ] 2.2 Grant access to resources based on job description and employee's need to know.

3.0 Change management

- [ ] 3.1 Create and document a formal change management process.
- [ ] 3.2 Establish a change review committee to examine and approve/reject proposed technology changes.

4.0 Backup and recovery

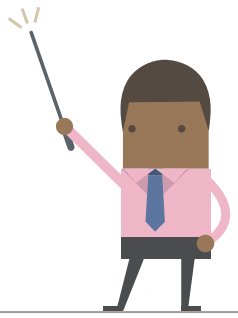
- [ ] 4.1 Create and document a data backup policy and ensure it is reviewed regularly.
- [ ] 4.2 Create and document a data recovery policy and ensure it is reviewed regularly.
- [ ] 4.3 Test data backup and recovery processes regularly.

5.0 Incident management

- [ ] 5.1 Create and document an approved companywide policy for incident response and management.
- [ ] 5.2 Test incident response procedures quarterly.

6.0 Information security

- [ ] 6.1 Create and document approved policies for information security and cybersecurity.
- [ ] 6.2 Protect network perimeters through a combination of firewalls and intrusion prevention systems.
- [ ] 6.3 Deploy and regularly test ransomware attack detection software.
- [ ] 6.4 Deploy antivirus software on all desktop devices and laptop computers.



SOURCE: PAUL KIRVAN. ILLUSTRATION: INUENG/GETTY IMAGES

TechTarget