IT GENERAL CONTROLS AUDIT TEMPLATE

This ITGC audit template evaluates an organization's security issues, management, and backup and recovery, and provides recommendations for how to move forward.
By Paul Kirvan

PHYSICAL & ENVIRONMENTAL SECURITY

	FINDINGS	RECOMMENDED ACTION
1. Server room is locked with a card access system.		
2. A limited number of employees have card access to the server room.		
3. The data center has raised floors and water detectors under the floors.		
4. An HVAC system alarm sends emails and launches audible signals if there is a system failure.		
5. Server room fire extinguishers are checked quarterly.		
6.		
7.		
8.		

LOGICAL SECURITY

	FINDINGS	RECOMMENDED ACTION
1. New employees are provided access to system resources after being approved by HR.		
2. Terminated employees have their access credentials deleted within 15 minutes of notification by HR.		
3. Windows Active Directory is used to authenticate users requesting system resources.		
4.		
5.		

CHANGE MANAGEMENT

	FINDINGS	RECOMMENDED ACTION
1. Test and production environments are segregated from each other.		
2. Production changes and patches are tested, documented and approved before being placed into service.		
3.		
4.		

BACKUP & RECOVERY

	FINDINGS	RECOMMENDED ACTION
1. Data is backed up daily according to a documented process and schedule.		
2. Disaster recovery plans are in place for critical systems, and are tested annually.		
3.		
4.		

INCIDENT MANAGEMENT

	FINDINGS	RECOMMENDED ACTION
1. Daily activity reports are generated for review by IT management.		
2. An incident response process is documented and used regularly when responding to abnormal situations.		
3.		
4.		

INFORMATION SECURITY

	FINDINGS	RECOMMENDED ACTION
1. Firewalls are used to protect the network perimeter from suspicious activities.		
2. Antivirus software is used to prevent damage from viruses.		
3. Incoming and outgoing data traffic are monitored 24/7 to identify potential phishing attacks, DDoS attacks and other attempts to penetrate the network perimeter.		
4. Penetration testing is performed twice annually to test for vulnerabilities.		
5.		
6.		

NEW CONTROL CATEGORY

	FINDINGS	RECOMMENDED ACTION
1.		
2.		
3.		