SOX404 Control Activities

Security

Governance

-Enterprise security policies, procedures and standards to support information integrity are documented and reviewed periodically.
-Segregation of duties between datacenter/hardware, network, operating system, application and data administration is documented and reviewed periodically.
-Segregation of duties between implementation, testing and authorization is documented and reviewed periodically.

Datacenter/Hardware

-Security changes are appropriately tested and authorized.
-Authorizers are reviewed periodically.
-Security is reviewed periodically.
-Activity is logged and monitored.

Network

-Security changes are appropriately tested and authorized.
-Authorizers are reviewed periodically.
-Security is reviewed periodically.
-Settings and configurations are reviewed and tested periodically.
-Non-standard activity is logged and monitored.
-External security appropriately protects the internal network.

Operating System

-Security changes are appropriately tested and authorized.
-Authorizers are reviewed periodically.
-Security is reviewed periodically.
-Settings and configurations are reviewed and tested periodically.
-Non-standard activity is logged and monitored.
-Anti-virus software is deployed on all desktops and servers and is maintained periodically.

Application

-Security changes are appropriately tested and authorized.
-Authorizers are reviewed periodically.
-Security is reviewed periodically.
-Settings and configurations are reviewed and tested periodically.

Data

-DBMS internal security vs. no internal security.
-Security changes are appropriately tested and authorized.
-Authorizers are reviewed periodically.
-Security is reviewed periodically.
-Settings and configurations are reviewed and tested periodically.
-Non-standard activity is logged and monitored.

Change Management

Governance

-Enterprise change management policies, procedures and standards to support information integrity are documented and reviewed periodically.
-Segregation of duties between datacenter/hardware, network, operating system, application and data administration is documented and reviewed periodically.
-Segregation of duties between implementation, testing and authorization is documented and reviewed periodically.

Datacenter/Hardware

-Changes are logged, tracked, documented, appropriately tested and authorized.
-Environments are separated based on job duties.
-Backout procedures are documented and available to the appropriate individuals.
-Authorizers are reviewed periodically.

Network

-Changes are logged, tracked, documented, appropriately tested and authorized.
-Types of changes include software upgrades & patches and configuration parameters.
-Environments are separated based on job duties.
-Backout procedures are documented and available to the appropriate individuals.
-Authorizers are reviewed periodically.

Operating System

-Changes are logged, tracked, documented, appropriately tested and authorized.
-Types of changes include software upgrades & patches and configuration parameters.
-Environments are separated based on job duties.
-Backout procedures are documented and available to the appropriate individuals.
-Authorizers are reviewed periodically.

Application

-Version control is maintained via migrations.
-Changes are logged, tracked, documented, appropriately tested and authorized.
-Types of changes include software upgrades & patches, internal development and configuration parameters.
-Environments are separated based on job duties.
-Backout procedures are documented and available to the appropriate individuals.
-Authorizers are reviewed periodically.

Data

-Internal change log vs. no internal change log.
-Changes are logged, tracked, documented, appropriately tested and authorized.
-Types of changes include software upgrades & patches, configuration parameters, database structure and data changes done outside secure, controlled and audited applications.
-Environments are separated based on job duties.
-Backout procedures are documented and available to the appropriate individuals.
-Authorizers are reviewed periodically.

Operations

Governance

-Enterprise operations policies, procedures and standards to support information integrity are documented and reviewed periodically.
-Segregation of duties between datacenter/hardware, network, operating system, application and data administration is documented and reviewed periodically.
-Segregation of duties between implementation, testing and authorization is documented and reviewed periodically.

Datacenter/Hardware

-Environmental controls appropriately protect equipment for temperature, humidity, power loss and fire suppression and are tested periodically.

Network

-Appropriate backups are done with media management, retention, secured off-site storage, auditing and testing of media.
-Requestors of backups must be authorized and authorizers are reviewed periodically.
-Schedule changes are authorized and authorizers are reviewed periodically.
-Non-standard events are recorded, analyzed and resolved in a timely manner.

Operating System

-Appropriate backups are done with media management, retention, secured off-site storage, auditing and testing of media.
-Requestors of backups must be authorized and authorizers are reviewed periodically.
-Schedule changes are authorized and authorizers are reviewed periodically.
-Non-standard events are recorded, analyzed and resolved in a timely manner.

Application

-Appropriate backups are done with media management, retention, secured off-site storage, auditing and testing of media.
-Requestors of backups must be authorized and authorizers are reviewed periodically.
-Schedule changes are authorized and authorizers are reviewed periodically.
-Non-standard events are recorded, analyzed and resolved in a timely manner.

Data

-Appropriate logging is enabled
-Appropriate backups are done with media management, retention, secured off-site storage, auditing and testing of media.
-Requestors of backups must be authorized and authorizers are reviewed periodically.
-Schedule changes are authorized and authorizers are reviewed periodically.
-Non-standard events are recorded, analyzed and resolved in a timely manner.