# SOX404 Control Objectives

## Change Management

### Governance
-The company-wide change management function is designed and implemented in a way that supports the information integrity objectives of the organization.
-Company-wide change management policies and procedures have been created and documented supporting the information integrity objectives of the organization.

### Hardware/Data Center
-Formal hardware change management process exists and is adequately documented.
-All hardware change requests raised are logged, tracked, and approved.
-Appropriate testing is performed for all changes. Testing procedures should include reviewing test results for expected results, approval of the test results, and appropriate documentation. (note: this may include testing of network software configurations critical to the hardware)
-Appropriate users are involved in testing changes, reviewing test results, and approving changes. Appropriate documentation of user testing exists.
-IT management reviews and approves all hardware changes and key deliverables prior to movement into production.
-Backout procedures exist for each change moved into production.
-The testing environment and the production environment appropriately restrict any unauthorized access.
-Emergency hardware changes are controlled and supervised by way of a documented emergency change procedure.

### Network
-A formal change management process is in place and is adequately documented for the network.
-All network change requests are logged, tracked, and approved prior to initiation of the change.
-All network changes are tested appropriately in a non-production environment. Testing procedures should include reviewing test results for expected results, approval of the test results, and appropriate documentation. Users should be involved in testing if appropriate based on the impact of the change.
-The test and production environments are appropriately restricted based on individuals' job functions.
-Back-out procedures are documented and available to the appropriate individuals for each change that is being moved into production.
-IT management reviews and approves all network changes and key deliverables prior to movement into production.
-Emergency network changes are controlled and supervised by way of a documented emergency change procedure.

## Security

### Governance
-The company-wide security function is designed and implemented in a way that supports the information integrity objectives of the organization.
-Company-wide security policy and procedures have been created and documented supporting the information integrity objectives of the organization.

### Hardware/Data Center
-Data center security management policies and procedures are in place and are adequately documented.
-Data center security is managed/owned by a group of qualified personnel separate from other Information Technology and Business Unit functions.
-A process is in place that requires appropriate approvals to add, modify, and delete user access to the data center commensurate with job responsibilities.
-Physical access is only granted to data center by way of appropriately restricted card key access.
-Data center access is logged and proactively monitored, and management takes any necessary subsequent action.

### Network
-Internal and external security management policies and procedures are in place and are adequately documented.
-Internal and external network security is managed by a group of qualified personnel separate from other Information Technology (IT) and Business Unit (BU) functions.
-Changes to internal and external network security settings and hardware configurations are reviewed, tested, and receive the appropriate approvals to ensure they are commensurate with their intended design.
-A process is in place that requires appropriate approvals to add, modify, and delete external network security access commensurate with job responsibilities.
-External network security access is monitored/reviewed on a regular basis to ensure it is granted, modified and deleted in a timely manner commensurate with job responsibilities.
-External network security measures appropriately protect the internal network from unauthorized access (DMZ, firewall placement and rule configuration, VPN access, and Encrypted communications).
-Potential security events are logged, monitored and management takes any necessary subsequent action.

## Operations

### Governance
-The company-wide operations function is designed and implemented in a way that supports the information integrity objectives of the organization.
-Company-wide operations policy and procedures have been created and documented supporting the information integrity objectives of the organization.

### Hardware/Data Center
-Operational policies, procedures and standards for establishing, maintaining and monitoring the operations of the data center exist and are documented.
-Non-standard operational events (run-time problems and exceptions from the pre-established schedule) are recorded, analyzed and resolved in a timely manner. This includes, but is not limited to, those routed through the help desk and identified in shift turnover logs.
-Operational responsibilities, as defined in organization charts, job descriptions, policies and procedures, are appropriately segregated from other IT and user responsibilities. Specifically: Operations personnel do not have programming, database administration, network administration, system administration, security administration or end user responsibilities.
-Scheduling changes, both permanent and temporary overrides, are properly authorized. Authorization levels and access rights are periodically reviewed.
-Environmental controls adequately protect equipment.
-Tape libraries are subject to regular audits. Backup tapes are periodically tested. Management reviews the list of authorized requestors and only those on the list can request backup tapes from the offsite storage. Associated policies and procedures are documented.

### Network
-Operational polices, procedures and standards for establishing, maintaining and monitoring the network exist and are documented.
-Non-standard network operational events (incidents, problems and errors) are recorded, analyzed and resolved in a timely manner. This includes, but is not limited to, those routed through the help desk.
-Operational responsibilities, as defined in organization charts, job descriptions, policies and procedures, are appropriately segregated from other IT and user responsibilities. Specifically: Network Administrators do not have computer operations, programming, database administration, operating system administration, security administration or end user responsibilities.
-Software, data and supporting documentation have adequate backup, media management (including future accessibility), record retention (per policies), and secured off-site storage.

# SOX404 Control Objectives

## Change Management - continued

**Operating System**
-A formal change management process is in place and is adequately documented for the various operating systems supporting the applications.
-All operating system change requests are logged, tracked, and approved prior to initiation of the change.
-All operating system changes are tested appropriately in a non-production environment. Testing procedures should include reviewing test results for expected results, approval of the test results, and appropriate documentation. Users should be involved in testing if appropriate based on the impact of the change.
-The test and production environments are appropriately restricted based on individuals' job functions.
-Back-out procedures are documented and available to the appropriate individuals for each change that is being moved into production.
-IT management reviews and approves all operating system changes and key deliverables prior to movement into production.
-Emergency operating system changes are controlled and supervised by way of a documented emergency change procedure.

**Application**
-Formal change management process exists and is adequately documented.
-All change requests raised are logged, tracked, and approved.
-Version control exists to ensure source code used is the most recent version and modifications by more than one programmer are coordinated.
-Code is modified / developed in an area separate from Test/Quality Assurance (QA) and Production.
-IT management reviews and approves program changes and key deliverables prior to movement into production.
-Appropriate users are involved in testing changes, reviewing test results, and approving changes. Appropriate documentation of user testing exists.
-Backout procedures exist for each change moved into the test / QA region and production environment.
-Procedures exist to ensure approved code from the test environment is migrated into production.
-Developers do not have write access to the test/QA environment or the production environment.
-Emergency changes are controlled and supervised by way of a documented emergency change procedure.

**Database**
-A formal change management process is in place and is adequately documented for the various databases supporting the applications.
-All database change requests are logged, tracked, and approved prior to initiation of the change.
-All database changes are tested appropriately in a non-production environment. Review procedures should include verifying that user-driven change requests contain evidence that user testing was performed and approved.
-The test and production environments are appropriately restricted to ensure appropriate segregation of duties.
-Back-out procedures are documented and available to the appropriate individuals for each change that is being moved into production.
-Database management reviews and approves all database changes and key deliverables prior to movement into production.
-Emergency database changes are controlled and supervised by way of a documented emergency change procedure.

## Security - continued

**Operating System**
-Security management policies and procedures are in place and are adequately documented.
-A process is in place that requires appropriate approvals to add, modify, and delete user OS access commensurate with job responsibilities.
-OS security access is monitored/reviewed on a regular basis to ensure it is granted, modified and deleted in a timely manner commensurate with job responsibilities.
-OS security is managed by a group of qualified personnel appropriately segregated from other Information Technology and Business Unit functions.
-OS activity is logged and monitored for unauthorized access on a regular basis and management takes any necessary subsequent action. Monitoring activities are segregated from security administration.
-OS security settings and configurations are reviewed on a regular basis and tested periodically to ensure they are commensurate with their intended design.
-Anti-virus software is deployed on all desktops, servers, and updated/employed on a regular basis.

**Application**
-Security Administration policies, procedures, and standards are in place and are adequately documented.
-A process is in place that requires appropriate management and data owner approvals to add, modify, and delete user access to applications, commensurate with job responsibilities.
-Application security access is monitored/reviewed on a regular basis to ensure it is granted, modified and deleted in a timely manner commensurate with job responsibilities.
-Application security is managed by a group of qualified personnel appropriately segregated from other Information Technology and Business Unit functions.

**Database**
-Security management policies and procedures governing direct access to data are in place and are adequately documented.
-A process is in place that requires appropriate approvals to add, modify, and delete direct access to data commensurate with job responsibilities.
-Direct access to data is monitored/reviewed on a regular basis to ensure it is granted, modified and deleted in a timely manner commensurate with job responsibilities.
-Data security is managed by a group of qualified personnel appropriately segregated from other Information Technology and Business Unit functions.
-Direct data access is logged and monitored for unauthorized access on a regular basis, and management takes any necessary subsequent action. Monitoring activities are segregated from security administration.

## Operations - continued

**Operating System**
-Operational polices, procedures and standards for establishing, maintaining and monitoring operating systems exist and are documented.
-Non-standard operating system operational events (incidents, problems and errors) are recorded, analyzed and resolved in a timely manner. This includes, but is not limited to, those routed through the help desk.
-Operational responsibilities, as defined in organization charts, job descriptions, policies and procedures, are appropriately segregated from other IT and user responsibilities. Specifically: Operating System Administrators do not have computer operations, programming, database administration, network system administration, security administration or end user responsibilities.
-Software, data and supporting documentation have adequate backup, media management (including future accessibility), record retention (per policies), and secured off-site storage.

**Application**
-Operational polices, procedures and standards for establishing, maintaining and monitoring the network exist and are documented.
-Non-standard network operational events (incidents, problems and errors) are recorded, analyzed and resolved in a timely manner. This includes, but is not limited to, those routed through the help desk.
-Operational responsibilities, as defined in organization charts, job descriptions, policies and procedures, are appropriately segregated from other IT and user responsibilities. Specifically: Application Administrators do not have computer operations, programming, database administration, network administration, operating system administration or security administration.
-Software, data and supporting documentation have adequate backup, media management (including future accessibility), record retention (per policies), and secured off-site storage.

**Database**
-Operational polices, procedures and standards for establishing, maintaining and monitoring the database exist and are documented.
-Non-standard database operational events (incidents, problems and errors) are recorded, analyzed and resolved in a timely manner. This includes, but is not limited to, those routed through the help desk.
-Operational responsibilities, as defined in organization charts, job descriptions, policies and procedures, are appropriately segregated from other IT and user responsibilities. Specifically: Database Administrators do not have computer operations, programming, network administration, operating system administration, security administration or end user responsibilities.
-Software, data and supporting documentation have adequate backup, media management (including future accessibility), record retention (per policies), and secured off-site storage.