QSoftware

Top Ten SOX / ITGC Controls (Summarized)

No.	Summarized Control	Q Cloud	On-Prem
1	**Access Provisioning** • Unique user-IDs are assigned/required for financially significant applications (system and/or generic accounts are permitted, provided there is a valid business need/purpose) • Request for add/change/delete users are documented, reviewed and approved, completed timely and the approver is different from the requestor • The request/assignment of incompatible duties that would compromise a segregation of duties (SOD) is prevented • Upon a workforce member changing job responsibilities, user access privileges are modified accordingly unless specific approval and duration for extension is provided • Terminated users are removed or disabled from the application in a timely manner		UAM
2	**Access Provisioning** • Administrator level and other privileged access (such as security configuration tables/tools) are restricted to a limited number of people • Activity performed using this access is logged and reviewed by supervisor level (where considered necessary)	x	UAM FD
3	**Access Reviews** • A periodic review of user access lists is performed by the business owner/representative to determine if the user should have access to the system and whether their access rights are appropriate based on the user's job roles and responsibilities • Reviews include: System Access, Privileged Access, Generic Account, Segregation of Duties		PR AM
4	**Passwords** • User authentication is required to access the system. Passwords meet minimum standards such as: a) Utilize an acceptable minimum password length where possible, and are passwords masked upon entry b) Are passwords required to be changed on a regular basis c) An acceptable password history usage standard is set d) Are users locked out after a pre-defined number of invalid logon attempts e) Is password complexity enabled		JDE
5	**Passwords** • Provide evidence showing the password for default accounts (such as JDE) have been changed		JDE
6	**Role Access Provisioning** • Request for add/change/delete of security within roles: a) Must be documented b) Must be reviewed and approved prior to making the change (in production) c) Approver must be different than requestor d) Must be completed timely		SMP

7	**Access** • All users/ids having elevated access (*ALL) in production are appropriate • Access to security functions / system administration is appropriately restricted to authorized accounts • Access to development, is restricted unless authorized/required • Access to batch processing functions (mass updates) is restricted unless authorized/required • Access to modify the Address Book which houses vendor and employee information is restricted unless authorized/required • The ability approve one's own 'batch' is restricted unless authorized/required	x	AM
8	**Access** • Job scheduler lists the time, name, description, etc. of all automated transactions. Exceptions in scheduled jobs and batch reports are reviewed by appropriate IT staff and issues are resolved in a timely manner. Evidence of review and issue resolution maintained by appropriate IT personnel	x	JDE AM
9	**Access** • Training and test accounts in production environment are authorized and required	x	AM
10	**Segregation of Duties** • Rule set is reviewed by the business on an annual basis to ensure all relevant objects are included. Changes to the rule set are documented and authorized	x	AM

The two right hand columns denote software which provides capabilities to process requests and/or provide evidence.

QCloud: 'x' in this column denotes capabilities exist in QCloud Security Audit

On-Prem: denotes capabilities exist in:

JDE	Standard JD Edwards
UAM	User Admin Manager
FD	Fraud Detector
PR	Periodic Review
SMP	Security Manager Pro
AM	Audit Manager

To find out more about Q Software solutions for managing
Security, Segregation of Duties and Audit in JD Edwards, visit www.qsoftware.com