Sarbanes-Oxley: Section 404

Electronic Records, Electronic Documents, Digital Signatures
White Paper

SoluSoft N2 WDMS Compliance with Sarbanes-Oxley: Section 404

The SOX requirements create an impact on corporate IT systems, practices and controls. It specifically affects data center operations, system software maintenance, application development and maintenance, business continuity and application software integrity. The critical area of IT control where the relevance of SOX is particularly high is in the control over application access through the use of identity and access management (IAM) processes and technologies.

The SOX legislation itself does not provide specific guidelines as to what is or is not an effective internal control. However, to provide some guidance to companies required to comply with SOX, the SEC identified the internal control framework developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) as one framework that meets its criteria.

As seen in Figure below, the COSO framework has three dimensions:

1. The nature of the control objectives i.e. operations, financial reporting, compliance
2. The organizational breadth of the company i.e., enterprise level, business unit level, activity / process level
3. The five components of effective internal control i.e. Control Environment, Risk Assessment, Control Activities, Information and Communication and Monitoring.

Figure 1. COSO Framework (source: COSO Internal Controls — Integrated Framework).

	Sarbanes-Oxley: Section 404 Compliance Requirement	Type of Requirement	Type	SoluSoft N2 Sarbanes-Oxley: Section 404 Compliance
1	**Central Identification, Authorization and Access Rights Management**	The logical access to and use of IT computing resources is restricted by the implementation of adequate identification, authentication and authorization mechanisms, linking users and resources to access rules.	Technical	N2 provides authentication and authorization. N2 integration with Microsoft Active Directory Services (ADS) provides central single sign for authentication. This method provides strong login and password controls with policies for the format, length, and re-use of user login and passwords with central user and N2 system resource management. The authorization uses roles and access control list (ACLs) to protect and prevent unauthorized access to database records, documents and system resources. The roles and ACLs are created as per company business procedures, rules, and regulations. Digital signature will provide strong non repudiation to maintain authenticity of records.
2	**Security of Online Access to Data**	In an online IT environment, IT management implement procedures in line with the security policy that provides access security control based upon the individual's need to view, add, change or delete data.	Technical	N2 provides authentication and authorization security of online access to system resources. The authorization uses roles and access control list (ACLs) to protect and prevent unauthorized access to database records, documents and system resources. The roles and ACLs are created as per company business rules, procedures and regulations.
3	**User Account**	Management may establish	Procedural	N2 Security Manager in conjunction

	Management	procedures to ensure timely action relating to requesting, establishing, issuing, suspending and closing of user accounts. A formal approval procedure outlining the data or system owner granting the access privileges should be included. The security of third-party access is defined contractually to address administration and nondisclosure requirements. .	Technical	with Microsoft Active Directory Service is designed specifically to address the challenges of user management i.e., requesting, establishing, issuing, suspending and closing of user accounts. Once a user has a user login id, whether it is a company officer, a business partner, an employee, or a casually interested customer, access to corporate resources can be managed while safeguarding proprietary resources. N2 provides an integrated workflow capability that can be used to manage user access requests through a formal and efficient approval process. N2 User Manager also provides a flexible, role-based, user administration capability that is used to more efficiently manage changes, suspensions and terminations to user access. Using N2 Security Manager, security policies can be defined and be enforced centrally to make sure that third-party access to applications is sufficiently controlled.
4	**Management Review of User Accounts**	Management may have a control process in place to review and confirm access rights periodically. Periodic comparison of resources with recorded accountability should be made to help reduce the risk of errors, fraud, misuse or unauthorized modification.		Auditing and reporting capabilities enable the review of user access privileges and how they have used those privileges in the past. An audit report can exhibit all user and site activity, including all authentications and authorizations, as well as administrative activity.

5	**Violation and Security Activity Reports**	IT security administration may ensure that security activity is logged and any indication of imminent security violation is reported immediately to all who may be concerned, internally and externally and is acted upon in a timely manner.	Technical Procedural	N2 access control tracks user sessions so administrators can monitor the resources being accessed, what and how often users attempt access to particular resources and how many users are accessing certain applications.
6	**Counter Party Trust**	Organizational policy may ensure that control practices are implemented to verify the authenticity of the counter-party providing electronic instructions and transactions.	Technical	N2 Single Sign-On in conjunction with Microsoft Active Directory provide for the management of various authentication technologies including passwords, tokens, X.509 certificates, custom forms secured socket layer access, and biometrics, as well as combinations of authentication methods.
7	**Transaction Authorization**	Organizational policy may ensure that, where appropriate, controls are implemented to provide authenticity of transactions and establish the validity of a user's claimed identity to the system.	Technical	N2 secures online transactions to ensure that the requestor is properly authorized. The authorization uses roles and access control list (ACLs) to protect and prevent unauthorized access to database records, documents and system resources. The roles and ACLs are created as per company business procedures, rules, and regulations. Additionally N2 supports strong encryption of data and control information that they process.
8	**Non-Repudiation**	Organizational policy may ensure that, where appropriate, neither party can deny transactions and controls are implemented to provide non repudiation of origin or receipt, proof of submission and receipt of transactions.	Technical	N2 in conjunction with Microsoft Active Directory (ADS) Single Sign-On support a wide range of authentication approaches to ensure that repudiation is a non issue. N2 and ADS authentication policies give security administrators unique management capabilities to mix and match authentication methods. N2 ensures transaction non-repudiation by recording every transaction so that a complete audit trail, including authorization and

				authentication information that is provided, is available in situations where repudiation could be an issue. This is implemented through Digital signatures, Time Stamping and extensive logs.
9	**Cryptographic Key Management**	Management may define and implement procedures and protocols to be used for generation, change, revocation, destruction, distribution, certification, storage, entry, use and archiving of cryptographic keys to ensure the protection of keys against modification and unauthorized disclosure.	Procedural Technical	N2 supports integration with Network Attached Storage (NAS), Storage Array Network (SAN) for storage scalability, archiving, encryption, and purging.
10	**Malicious Software Prevention, Detection, and Correction**	Management may define and implement procedures to ensure that critical systems are not vulnerable to malicious software such as viruses and other attacks.	Technical Procedural	*Third party* Integrated Threat Management provides comprehensive antivirus, anti-spyware, intrusion detection, surf protection, firewall capabilities. N2 Access Control also provides self-integrity checking, so that Trojan horse access control components cannot be introduced into an environment.