White Paper

Regulatory Compliance and Database Management

March 2006

Introduction

Top of mind in business executives today is how to meet new regulatory compliance and corporate governance. New laws are changing the way companies collect, retain, and manage information. DBAs need to understand what is happening in the corporate business world and how it will directly impact their job role.

As each new year arrives, it brings with it new challenges for IT organizations that support business. Whether a new calendar year with renewed budgets or start of a new quarter, there are sure to be new projects for IT. Almost assured, one of the projects at the top of the list will be one of regulatory compliance as the time grows near for company executives to again verify compliance with the Sarbanes-Oxley Act (SOX). Section 404 of the SOX Act mandates that executive management of publicly held companies must evaluate and report on the effectiveness of their internal controls over financial reporting, and have independent auditors substantiate the effectiveness of the procedures and internal controls for financial reporting.

Complying to New Regulations

Although the primary purpose of SOX is to assure corporate governance standards of financial reporting and auditing, wider interpretation can include IT operational processes that support a business. Company's executives are now reaching out to IT to access and provide record of policies, process, and procedures that control access and protect the integrity of financials systems and business applications, across networks, servers and into databases where the data is stored. As IT organizations start to address SOX, questions are being raised on how far does it reach, what is affected, and what should be reviewed and reported. Although there is guidance available from various sources, there has yet to appear a definitive set of guidelines that is not open to interpretation. Offered only as examples to assist in meeting compliance, here are five potential ways an organization might fail an upcoming audit if not properly prepared:

- No security management or demonstration of security for systems of financial record or systems that could affect financial systems integrity. Companies must assure that financial information is safe from unauthorized outside or internal influences.
- Not having documented procedures, records or changes, or auditable demonstration of change management when System, Database, and Network Administrators make alterations or updates on systems of financial record or those systems that could affect financial systems integrity. Proper change management must exist to ensure that software and hardware changes are controlled and recorded.
- No documented disaster recovery plan or auditable verification of successful plan execution of recoverability of systems of financial record. This includes demonstrating recoverability of financial systems for reasonable business continuance with minor business impact. No matter the size or the complexity of the system, organizations must assure recovery within a period of time that ensures availability of financial data in a timely manner.
- Database logging not enabled, logs not secured, no reporting of database transactions, or demonstration of log audit reporting for financial systems of record or systems that could affect financial systems integrity. Without database logging and log reporting, it next to impossible to identify who changed what in the database. Database Administration change management comparisons should be verified against database log reports to ensure all database alterations are recorded and verifiable.
- Backups or data movement onto disk, tape, or stored at third-party sites is not secured and tracked. Unsecured financial data can be vulnerable to theft, unauthorized viewing, or alteration. For instance, a Transportable Tablespace of a database could potentially be moved and reattached to another database enabling unauthorized viewing. Database archival, backups, loading and unloading, administration change management and reporting should be performed and routinely verified to ensure that data is secured.

SOX section 404’s requires an external auditor’s opinion on the effectiveness of internal controls. For audit, and quarterly certification, companies need to demonstrate what control changes are implemented to attest to integrity, confidentiality and non-repudiation of financial reporting. If process controls can be bypassed, executive management cannot with certainty sign off on the adequacy of controls for financial data integrity.

As SOX legislation is relatively new and affects a majority of companies today, the SEC has identified guidelines provided by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) in evaluating internal controls. IT control requirements are most often derived from SOX regulation internal controls sections 302 and 404.

While (COSO) does provides a general framework for accounting internal controls, but not IT specific, organizations can find IT specific models available within the Control Objectives for Information and related Technology (COBIT®) to assist with SOX compliance. Created by Information Technology Governance Institute (ITGI) **www.itgi.org**, the COBIT Framework provides control objectives focusing on the processes specific to the IT environment.

COBIT aligns with the general COSO framework with internal controls consisting of 4 domains, 34 processes and over 225 detailed control objectives aligning with the IT implementation cycle. The Domains are Planning and Organization, Acquisition and Implementation, Delivery and Support, and Monitor and Evaluate. A few examples of the processes defined that address the enterprise data environment are:

- Acquire and Maintain Application Software
- Acquire and Maintain Technology Infrastructure
- Ensure Systems Security
- Manage the Configuration
- Manage Problems and Incidents
- Manage Data
- Manage Operations

COBIT key controls and questions assist in measurement and assessment of current processes, process control objectives, success criteria for process implementation and metrics to evaluate and quantifying process improvement. Guidelines help drive IT governance and compliance by aligning IT decisions with business strategy.

Key controls in COBIT include such activities as:

- Separation of duties
- Effective change management
- Effective change documentation
- Release Processes
- Control Processes
- Resolution Processes

Key Questions a DBA Should Be Prepared to Answer/Demonstrate

By no means a definitive list or one that assures compliance, these sample questions can help ascertain your data and database management knowledge on the subject matter in preparation for audit. At a minimum, DBAs should be reviewing their practices for database archival, backups, loading and unloading, administration change management and reporting.

- Have data integrity ownership and responsibilities been communicated to appropriate data/business owners and their acceptance of responsibilities?
- Are key database systems inventoried, owners identified and documented:
  — Number of databases and instances
  — Type and version of the database software installed
  — Type and version of the underlying operating system
  — Database users and privileges compared with user system security
  — Related applications accessing or transacting with the database (e.g., ERP, web, custom)
  — Utilities and tools that can access, manage, or change the database or data
  — Organization charts identifying system owners and maintainers
- Do you have Change Management in place so you can you attest to any changes or alterations?
- Where are the risks to financial data stored in databases documented? How often are they reviewed and updated?
- Is the data that is extracted, archived, or backed up, properly secured and tracked?
- How are division of roles and responsibilities (segregation of duties) setup so that it prevents a Database Administrator (DBA) from unauthorized data viewing, alterations, or deletions?
- What are the Database Management process controls? Where are they documented for review? What monitoring and reporting do you have in place? Can you demonstrate this (pick randomly) one to me now?
- When was the last time the Database Management control methods were tested, gaps identified and controls improved?
- Do you understand and accept the responsibility regarding internal controls for the databases you manage?

Before your executive management signoffs on SOX, what processes has your IT department put in place to prevent authorized users from accessing, altering, accidentally or deliberately deleting data that could result in incorrect financial reporting? Are you prepared when an auditor asks, "where are your documented processes and can you demonstrate them"? Are those processes just what it takes to pass an initial audit, or industry standard practices like COBIT that are repeatable and supportable when resources move on to other roles or depart the company? If not, then now is the time to kick-off a project to have them addressed.

Preparing For Audit

Auditors are seeking validation that the DBMS maintains accurate and reliable data, control of objects and data is by authorized users only, and proper backup and data restoration is provided. Organizations need to have controls to ensure that qualified DBAs:

- Are responsible for ensuring database retains financial data integrity and are accountable if a database is compromised

- Track and approve all database modifications and manage the security of the database by the proper roles and access management

- Validate database backup and recovery of the largest of databases within a "reasonable time" to meet business continuance audit criteria.

In preparation for a best practice review or audit, DBAs should:

1. Perform active discovery daily and maintain an inventory of all financial system databases, databases with which they exchange data, and databases objects associated with financial data

2. Establish and document repeatable best practices for database change management: for managing object permissions, schema changes, roles and privileges to eliminate risk of unauthorized viewing, altering, or copying of data

3. Ensure protection of database transaction logs from alteration and deletion, perform database log audit validation of databases changes and implement proactive log analysis and rapid corrective action and when unauthorized changes occur

4. Conduct database backups or exports, and routinely verify data is secured and can demonstrate recoverability within reasonable period of time for business continuance

For those companies with large and complex databases or even a number of different database types, the four tasks listed above could quickly overcome data or database administration staff if performed manually. If custom coding and scripts are considered for automation and not commercial off-the-shelf software, the extra time, resources, and cost to support continuous development, code management and repudiation to auditors should be considered as part of budget planning.

CA Provides Technology for Your Regulatory Compliance Efforts

CA offers comprehensive management solutions that can help you reduce the total cost of ownership, manage day-to-day operations and increase overall service management and compliance.

CA's Unicenter® Asset Management Solutions enables customers to automate discovery and maintain an inventory of IT assets including databases. It automates critical IT management processes, including discovery of network assets, inventory, maintenance activities, license administration and cross-platform reporting. For more on CA Asset Management, please visit **ca.com/assetmanagement**.

CA's Unicenter® Database Administration Solutions automate DBA's day-to-day tasks such as multi-database schema management, database security, Referential Integrity management, and catalog administration, allowing the DBA to maintain control of the database environment. Controlled automation delivers higher-quality change management and change control while reducing the DBA's workload. For more on CA Database Management, please visit **ca.com/databasemanagement**.

CA's AllFusion® Modeling Suite Solutions design task optimization combined with robust documentation and impact analysis capabilities can provide significant portions of the infrastructure to satisfy these compliance requirements. For more on CA Database Management, please visit **ca.com/databasemanagement**.

CA's BrightStor® ARCserve® Backup and Unicenter® Database Backup and Recovery Solutions are fast, safe and cost-effective solutions to automate routine backups, avoid failures, and recover databases when problems do occur. Even without a major disaster, when errors or people corrupt or lose critical data, or it becomes unavailable for an extended period of time, it can have a significant impact on a company's profitability. For more on CA BrightStor ARCserve Backup, please visit **ca.com/brightstor**.

CA's Unicenter® Log Analyzer Solutions decode proprietary database log files and enable transaction log analysis remotely without the overhead of log auditing analysis internal to the databases or on the local system. It enables DBAs to automate database log auditing, undo or redo specific changes, and analyze transaction-level detail to reduce data loss or troubleshoot application performance problems. For more on CA Database Management, please visit **ca.com/databasemanagement**.

Based on the COBIT control framework, the following grid provides greater detail on CA Database Management Solutions that can assist on SOX section 404 compliance.

CA Unicenter Database Management Solutions and COBIT

Plan and Organize		Definition	CA Database Management Products That Assist
PO2	**Define the Information Architecture**	The information systems function should create and regularly update a business information model and define the appropriate systems to optimize the use of this information.	
PO2.1	Enterprise Information Architecture Model	Establish and maintain an enterprise information model to enable applications development and decision-supporting activities, consistent with IT plans.	• AllFusion® ERwin® Data Modeler • AllFusion® Data Model Validator • AllFusion® Saphir Option • AllFusion® Model Manager
PO2.2	Enterprise Data Dictionary and Data Syntax Rules	Maintain an enterprise data dictionary that incorporates the organization's data syntax rules.	• Unicenter® Database Administration
PO2.3	Data Classification Scheme	Establish a classification scheme that applies throughout the enterprise, based on the criticality and sensitivity (e.g., public, confidential, top secret) of enterprise data.	• AllFusion ERwin Data Modeler
PO2.4	Integrity Management	Define and implement procedures to ensure integrity and consistency of all data stored in electronic form, such as databases, data warehouses and data archives.	• Unicenter Database Administration
PO4	**Define the IT Processes, Organization and Relationships**	An IT organization must be defined considering requirements for staff, skills, functions, accountability, authority, roles and responsibilities, and supervision. Processes, administrative policies and procedures need to be in place for all functions, with specific attention to control, quality assurance, risk management, information security, data and systems ownership, and segregation of duties.	
PO4.6	Roles and Responsibilities	Define and communicate roles and responsibilities for all personnel in the organization in relation to information systems to allow sufficient authority to exercise the role and responsibility assigned to them.	• Unicenter Database Administration — assists in role identification for audit
PO4.9	Data and System Ownership	Provide the business with procedures and tools enabling it to address its responsibilities for ownership of data and information systems.	• Unicenter Database Administration
PO4.10	Supervision	Implement adequate supervisory practices in the IT function to ensure that roles and responsibilities are properly exercised, to assess whether all personnel have sufficient authority and resources to execute their roles and responsibilities, and to generally review key performance indicators.	• Unicenter Database Administration • Unicenter® Database Performance Management
PO4.11	Segregation of Duties	Implement a division of roles and responsibilities that reduces the possibility for a single individual to subvert a critical process. Management also makes sure that personnel are performing only authorized duties relevant to their respective jobs and positions.	• Unicenter Database Administration

Acquire and Implement		**Definition**	**CA Database Management Products That Assist**
AI2	**Acquire and Maintain Application Software**	Applications have to be made available in line with business requirements. This process covers the design of the applications, the proper inclusion of application controls and security requirements, and the actual development and configuration according to standards.	
AI2.1	High-level Design	Translate business requirements into a high-level design specification for software development, taking into account the organization's technological directions and information architecture, and have the design specifications approved to ensure that the high-level design responds to the requirements.	▪ AllFusion Modeling Suite
AI2.2	Detailed Design	Prepare detailed design and technical software application requirements. Perform reassessment when significant technical or logical discrepancies occur during development or maintenance.	▪ AllFusion Modeling Suite
AI2.3	Application Control and Auditability	Ensure that business controls are properly translated into application controls such that processing is accurate, complete, timely, authorized and auditable. Issues to consider especially are authorization mechanisms, information integrity, access control, backup and design of audit trails.	▪ Unicenter® Log Analyzer
AI2.4	Application Security and Availability	Address application security and availability requirements in response to identified risks, in line with data classification, the organization's information security architecture and risk profile. Issues to consider include access rights and privilege management, protection of sensitive information at all stages, authentication and transaction integrity, and automatic recovery.	▪ Unicenter Log Analyzer ▪ Unicenter® Database Backup and Recovery
AI2.5	Configuration and Implementation of Acquired Application Software	Customize and implement acquired automated functionality using configuration, acceptance and testing procedures. Issues to consider include validation against contractual terms, the organization's information architecture, existing applications, interoperability with existing application and database systems, system performance efficiency, documentation and user manuals, integration and system test plans.	▪ Unicenter Database Administration ▪ Unicenter® SQL-Station® ▪ Unicenter® SQL-Ease®
AI2.6	Major Upgrades to Existing Systems	Follow a similar development process as for the development of new systems in the event of major changes to existing systems that result in significant change in current designs and/or functionality.	▪ Unicenter SQL-Station ▪ Unicenter SQL-Ease
AI2.7	Development of Application Software	Ensure that automated functionality is developed in accordance with design specifications, development and documentation standards and quality requirements. Issues to be considered include approval that design specifications meet business, functional and technical requirements; approval of change requests; and confirmation that application software is compatible with production and ready for migration.	▪ Unicenter SQL-Station ▪ Unicenter SQL-Ease
AI2.8	Software Quality Assurance	Develop resource and execute a software quality assurance plan to obtain the quality specified in the requirements definition and the organization's quality policies and procedures. Issues to consider in the quality assurance plan include specification of quality criteria and validation and verification processes, including inspection, walkthroughs and testing.	▪ Unicenter SQL-Station ▪ Unicenter SQL-Ease

Acquire and Implement		Definition	CA Database Management Products That Assist
AI2.10	Application Software Maintenance	Develop a strategy and plan for the maintenance and release of software applications. Issues to consider include release planning and control, resource planning, bug fixing and fault correction, minor enhancements, maintenance of documentation, emergency changes, interdependencies with other applications and infrastructure, upgrade strategies, contractual conditions such as support issues and upgrades, periodic review against business needs, risks and security requirements.	▪ Unicenter SQL-Station ▪ Unicenter SQL-Ease ▪ Unicenter Database Administration
AI3	**Acquire and Maintain Technology Infrastructure**	Organizations should have processes for the acquisition, implementation and upgrade of the technology infrastructure. This requires a planned approach to acquisition, maintenance and protection of infrastructure in line with agreed technology strategies and the provision of development and test environments.	
AI3.2	Infrastructure Resource Protection and Availability	Implement internal control, security and auditability measures during configuration, integration and maintenance of hardware and infrastructural software to protect resources and ensure availability and integrity. Responsibilities for using sensitive infrastructure components should be clearly defined and understood by those who develop and integrate infrastructure components. Their use should be monitored and evaluated.	▪ Unicenter Database Performance Management ▪ Unicenter Database Administration ▪ Unicenter Log Analyzer ▪ Unicenter Database Backup and Recovery
AI3.3	Infrastructure Maintenance	Develop a strategy and plan for infrastructure maintenance and ensure that changes are controlled in line with the organization's change management procedure. Include periodic review against business needs, patch management and upgrade strategies, risks, vulnerabilities assessment and security requirements.	▪ Unicenter Database Administration
AI3.4	Feasibility Test Environment	Establish development and test environments to support effective and efficient feasibility and integration testing of applications and infrastructure in the early stages of the acquisition and development process. Consider functionality, hardware and software configuration, integration and performance testing, migration between environments, version control, test data and tools, and security.	▪ Unicenter SQL-Station ▪ Unicenter SQL-Ease ▪ Unicenter Database Administration
AI4	**Enable Operation and Use**	Knowledge about new systems needs to be made available. This process requires the production of documentation and manuals for users and IT, and provides training to ensure proper use and operations of applications and infrastructure.	
AI4.1	Planning for Operational Solutions	Develop a plan to identify and document all technical aspects, operational capability and required service levels, so all stakeholders can take timely responsibility for the production of management, user and operational procedures, as a result of the introduction or upgrade of automated systems or infrastructure.	▪ Unicenter Database Performance Management
AI4.2	Knowledge Transfer to Business Management	Transfer knowledge to business management to allow them to take ownership of the system and data and exercise responsibility for service delivery and quality, internal control, and application administration processes. The knowledge transfer should include access approval, privilege management, segregation of duties, automated business controls, backup/recovery, physical security and source document archival.	▪ Unicenter Database Administration ▪ Unicenter Database Backup and Recovery

Acquire and Implement		Definition	CA Database Management Products That Assist
AI4.3	Knowledge Transfer to End Users	Transfer knowledge and skills to allow end users to effectively and efficiently use the application system to support business processes. The knowledge transfer should include the development of a training plan to address initial and ongoing training and skills development, training materials, user manuals, procedure manuals, online help, service desk support, key user identification, and evaluation.	▪ Unicenter Database Administration ▪ Unicenter Database Backup and Recovery
AI4.4	Knowledge Transfer to Operations and Support Staff	Transfer knowledge and skills to enable operations and technical support staff to effectively and efficiently deliver, support and maintain the application system and associated infrastructure according to required service levels. The knowledge transfer should include initial and ongoing training and skills development, training materials, operations manuals, procedure manuals, and service desk scenarios.	▪ Unicenter Database Administration ▪ Unicenter Database Backup and Recovery
AI6	**Manage Changes**	All changes, including emergency maintenance and patches, relating to infrastructure and applications within the production environment must be formally managed in a controlled manner. Changes (including procedures, processes, system and service parameters) must be logged, assessed and authorized prior to implementation and reviewed against planned outcomes following implementation.	
AI6.1	Change Standards and Procedures	Set up formal change management procedures to handle in a standardized manner all requests (including maintenance and patches) for changes to applications, procedures, processes, system and service parameters, and the underlying platforms.	▪ Unicenter Database Administration
AI6.4	Change Status Tracking and Reporting	Establish a tracking and reporting system for keeping change requestors and relevant stakeholders up to date about the status of the change to applications, procedures, processes, system and service parameters, and the underlying platforms.	▪ Unicenter Database Administration ▪ Unicenter SQL-Station
AI7	**Install and Accredit Solutions and Changes**	New systems need to be made operational once development is complete. This requires proper testing in a dedicated environment with relevant test data, definition of rollout and migration instructions, release planning and actual promotion to production, and a post-implementation review.	
AI7.4	Test Environment	Establish a separate test environment for testing. This environment should reflect the future operations environment (e.g., similar security, internal controls and workloads) to enable sound testing. Procedures should be in place to ensure that the data used in the test environment are representative of the data that will eventually be used in the production environment.	▪ Unicenter SQL-Station ▪ Unicenter SQL-Ease ▪ Unicenter® Fast Unload ▪ Unicenter Database Administration
AI7.5	System and Data Conversion	Ensure that the organization's development methods provides for all development, implementation or modification projects, that all necessary elements such as hardware, software, transaction data, master files, backups and archives, interfaces with other systems, procedures, system documentation, etc., be converted from the old system to the new according to a pre-established plan. An audit trail of pre- and post-conversion results should be developed and maintained.	▪ Unicenter Database Administration ▪ Unicenter Fast Unload ▪ Unicenter Database Backup & Recovery ▪ Unicenter Log Analyzer

Acquire and Implement		Definition	CA Database Management Products That Assist
AI7.6	Testing of Changes	Ensure that changes are tested in accordance with the defined acceptance plan and based on an impact and resource assessment that includes performance sizing in a separate test environment by an independent (from builders) test group before use in the regular operational environment begins. The security controls should be tested and evaluated prior to deployment, so the effectiveness of security can be certified. Fallback/backout plans should also be developed and tested prior to promotion of the change to production.	▪ Unicenter Database Administration ▪ Unicenter Fast Unload ▪ Unicenter Database Backup & Recovery ▪ Unicenter Log Analyzer
AI7.7	Final Acceptance Test	Ensure that procedures provide for, as part of the final acceptance or quality assurance testing of new or modified information systems, a formal evaluation and approval of the test results by management of the affected user department(s) and the IT function. The tests should cover all components of the information system (e.g., application software, facilities, technology and user procedures) and ensure that the information security requirements are met by all components. The test data should be saved for audit trail purposes and for future testing.	▪ Unicenter Database Administration ▪ Unicenter Fast Unload ▪ Unicenter Database Backup & Recovery ▪ Unicenter Log Analyzer
AI7.8	Promotion to Production	Implement formal procedures to control the handover of the system from development to testing to operations in line with the implementation plan. Management should require that system owner authorization be obtained before a new system is moved into production and that, before the old system is discontinued, the new system has successfully operated through all daily, monthly, quarterly and year-end production cycles.	▪ Unicenter Database Administration ▪ Unicenter Fast Unload ▪ Unicenter Database Backup & Recovery ▪ Unicenter Log Analyzer
AI7.9	Software Release	Ensure that the release of software is governed by formal procedures ensuring sign-off, packaging, regression testing, distribution, handover, status tracking, backout procedures and user notification.	▪ Unicenter Database Administration ▪ Unicenter Database Backup & Recovery ▪ Unicenter SQL-Station
AI7.11	Recording and Tracking of Changes	Automate the system used to monitor changes to application systems to support the recording and tracking of changes made to applications, procedures, processes, system and service parameters, and the underlying platforms.	▪ Unicenter Database Administration ▪ Unicenter Log Analyzer
Deliver and Support		**Definition**	**CA Database Management Products That Assist**
DS1	**Define and Manage Service Levels**	Effective communication between IT management and business customers regarding services required is enabled by a documented definition and agreement of IT services and service levels. This process also includes monitoring and timely reporting to stakeholders on the accomplishment of service levels.	
DS1.5	Monitoring and Reporting of Service Level Achievements	Continuously monitor specified service level performance criteria. Reports are provided in a format meaningful to the stakeholders on achievement of service levels. The monitoring statistics are analyzed and acted upon to identify negative and positive trends for individual services as well as for services overall.	▪ Unicenter Database Performance Management

Deliver and Support		Definition	CA Database Management Products That Assist
DS3	**Manage Performance and Capacity**	The need to manage performance and capacity of IT resources requires a process to periodically review current performance and capacity of IT resources. This process includes forecasting future needs based on workload, storage and contingency requirements.	
DS3.1	Performance and Capacity Planning	Establish a planning process for the review of performance and capacity of IT resources to ensure that cost-justifiable capacity and performance are available to process the agreed-upon workloads as determined by the service level agreements.	▪ Unicenter Database Performance Management
DS3.2	Current Capacity and Performance	Review current performance and capacity of IT resources to determine if sufficient capacity and performance exist to deliver against service level agreements.	▪ Unicenter Database Performance Management
DS3.3	Future Capacity and Performance	Conduct performance and capacity forecasting of IT resources at regular intervals to minimize the risk of service disruptions due to insufficient capacity or performance degradation. Also identify excess capacity for possible redeployment. Identify workload trends and determine forecasts to be input to performance and capacity plans.	▪ Unicenter Database Performance Management
DS3.4	IT Resources Availability	Provide the required capacity and performance taking into account aspects such as normal workloads, contingencies, storage requirements and IT resource life cycles. Provisions should be made when performance and capacity are not up to the required level such as prioritizing tasks, fault tolerance mechanisms and resource allocation practices.	▪ Unicenter Database Performance Management
DS3.5	Monitoring and Reporting	Continuously monitor the performance and capacity of IT resources. To maintain and tune current performance within IT and address such issues as resilience, contingency, current and projected workloads, storage plans and resource acquisition. To report delivered service availability to the business as required by the SLAs.	▪ Unicenter Database Performance Management
DS4	**Ensure Continuous Service**	The need for providing continuous IT services requires developing, maintaining and testing IT continuity plans, offsite backup storage and periodic continuity plan training. An effective continuous service process minimizes the probability and impact of a major IT service interruption on key business functions and processes.	
DS4.9	Offsite Backup Storage	Store offsite all critical backup media, documentation and other IT resources necessary for IT recovery and business continuity plans. Management of the offsite storage facility should respond to the data classification policy and the enterprise's media storage practices.	▪ Unicenter Database Backup and Recovery
DS5	**Ensure Systems Security**	The need to maintain the integrity of information and protect IT assets requires a security management process. This process includes establishing and maintaining IT security roles and responsibilities, policies, standards and procedures.	

Deliver and Support		Definition	CA Database Management Products That Assist
DS5.4	User Account Management	Ensure that requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges are addressed by user account management. These procedures should apply for all users, including administrators (privileged users), internal and external users, for normal and emergency cases. Perform regular management review of all accounts and related privileges.	▪ Unicenter Database Administration
DS11	**Manage Data**	Effective data management requires identifying data requirements. The data management process also includes establishing effective procedures to manage the media library, backup and recovery of data, and proper disposal of media.	
DS11.2	Storage and Retention Arrangements	Define and implement procedures for data storage and archival, so data remain accessible and usable. Establish storage and retention arrangements to satisfy legal, regulatory and business requirements for documents, data, archives, programs, reports and messages (incoming and outgoing) as well as the data (keys, certificates) used for their encryption and authentication.	▪ Unicenter Database Backup and Recovery
DS11.5	Backup and Restoration	Define and implement procedures for backup and restoration of systems, data and documentation in line with business requirements and the continuity plan. Verify compliance with the backup procedures, and verify the ability to and time required for successful and complete restoration. Test backup media and the restoration process.	▪ Unicenter Database Backup and Recovery ▪ Unicenter Log Analyzer
DS11.6	Security Requirements for Data Management	Establish arrangements to identify and apply security requirements for receipt, processing, physical storage and output of data and sensitive messages. This includes physical records, data transmissions and data offsite.	▪ Unicenter Database Backup and Recovery
DS13	**Manage Operations**	Complete and accurate processing of data requires effective management of data processing and maintenance of hardware. This process includes defining operations' policies and procedures for effective management of scheduled processing, protection of sensitive output, monitoring infrastructure and preventative maintenance of hardware.	
DS13.3	IT Infrastructure Monitoring	Define and implement procedures to monitor the IT infrastructure and related events. Ensure sufficient chronological information is being stored in operations logs to enable the reconstruction, review and examination of the time sequences of operations and the other activities surrounding or supporting operations.	▪ Unicenter Database Performance Management
DS13.5	Preventive Maintenance for Hardware	Define and implement procedures to ensure timely maintenance of infrastructure to reduce the frequency and impact of failures or performance degradation.	▪ Unicenter Database Performance Management

Monitor and Evaluate		Definition	CA Database Management Products That Assist
ME1	**Monitor and Evaluate IT Performance**	Effective IT performance management requires a monitoring process. This process includes defining relevant performance indicators, a systematic and timely reporting of performance, and prompt acting upon deviations. Monitoring is needed to make sure that the right things are done and are in line with the set directions and policies.	
ME1.3	Monitoring Method	Ensure that the monitoring process deploys a method (e.g., balanced scorecard) that provides a succinct, all-around view of IT performance and fits within the enterprise monitoring system.	Unicenter® Database Command Center

Summary

SOX does not mandate software; however, technology and automation can be used to ease the amount of work and cost of compliance as compared to manual or paper-based methods.

Auditors will be seeking documentation and demonstration of consistent and repeatable processes and controls. Instead of taking the risk of a failed audit, the rising cost of maintaining manual controls as data volumes increase database size and complexity, or re-evaluations caused by business changes you can instead choose a software solution from CA to automate and improve controls in a consistent and efficient manner. CA provides tools to help meet requirements, and help the various stakeholders in your organization understand and feel confident in their internal financial controls. URLs for additional reference and detail:

Industry Organizations

- isaca.org
- coso.org
- auditnet.org/sox.htm
- itgi.org/
- aicpa.org/news/2004/2004_0929.htm

CA Technology

- ca.com/compliance
- ca.com/databasemanagement

Quality System
Quality
Endorsed
Company
ISO 9001
Lic. 2443

MP297230306