Comply with specific regulations

IDERA SQL Compliance Manager audits and identifies events that affect SQL Server objects and data. By selecting a specific regulation guideline set, SQL Compliance Manager applies audit settings to your selected databases according to the corresponding data security rules. This audited data is collected and securely stored for forensic analysis and reporting. SQL Compliance Manager also provides tamper-proof data security features as well as methods for watching events without exposing account information.

You can apply a regulation guideline when you register a new SQL Server instance or audit a database through the Console or CLI. The following tables list each section of a regulation and the associated SQL Server events that SQL Compliance Manager audits, as well as specific audit features.

IDERA, Inc. customers have the sole responsibility to ensure their compliance with the laws and standards affecting their business. IDERA, Inc. does not represent that its products or services ensure that customer is in compliance with any law. It is the responsibility of the customer to obtain legal, accounting, or audit counsel as to the necessary business practices and actions to comply with such laws.

All Regulation Guidelines are available at both, the server level and the database level, except for the CIS Regulation Guideline.

The CIS Regulation Guideline can be applied only at the server level.

CIS Compliance

Section	Summary	Associated Audit Events and Features
5.4	Ensure 'SQL Server Audit' is set to capture both 'failed' and 'successful logins'. SQL Server Audit is capable of capturing both failed and successful logins and writing them to one of three places: the application event log, the security event log, or the file system. We will use it to capture any login attempt to SQL Server, as well as any attempts to change audit policy. This will also serve as a second source to record failed login attempts.	Server Events: • Logins • Logouts • Failed Logins Database Events: • None

When selecting CIS regulation, default database level settings automatically apply. Logins and Failed Logins get captured to comply with this regulation and continue auditing the server.

DISA/STIG Compliance

Section	Summary	Associated Audit Events and Features

DISA 2016 Database **DISA 2016 Instance** SQL6-D0-004300, SQL6-D0-004500, SQL6-D0-004700, SQL6-D0-004800, SQL6-D0-005500, SQL6-D0-005900, SQL6-D0-006000, SQL6-D0-006100, SQL6-D0-006200, SQL6-D0-006300, SQL6-D0-006400, SQL6-D0-010700, SQL6-D0-010800, SQL6-D0-011100, SQL6-D0-011200	SQL Server must be configured to generate audit records for DoD-defined auditable events within all DBSM /database components. SQL Server must generate audit records when privileged/permissions are retrieved. SQL Server must initiate session auditing upon startup. SQL Server must be configured to allow authorized users to capture, record, and log all content related to a user session. SQL Server must include additional, more detailed, organization-defined information in the audit records for audit events identified by type, location, or subject. The audit information produced by SQL Server must be protected from unauthorized read access. The audit information produced by SQL Server must be protected from unauthorized modification. The audit information produced by SQL Server must be protected from unauthorized deletion. SQL Server must protect its audit features from unauthorized access. SQL Server must protect its audit configuration from unauthorized modification. SQL Server must protect its audit features from unauthorized removal. SQL Server must utilize centralized management of the content captured in audit records generated by all components of SQL Server. SQL Server must provide an immediate real-time alert to appropriate support staff of all audit failure events requiring real-time alerts. SQL Server must record time stamps in audit records and application data that can be mapped to Coordinate Universal Time (UTC, formerly GMT).	Server Events: • Successful and Failed Logins • Security Changes • Privileged User Activity • User Defined Event Tracking Database Events: • Security changes • SELECT statements • Privileged User Activity • Sensitive Column Monitoring • Before-After Data Auditing

DISA 2012 Database SQL2-00-011200 **DISA 2014 Database** SQL4-00-011200	SQL Server must generate Trace or audit records for organization-defined auditable events. Audit records can be generated from various components within the information system.	Server Events: • None Database Events: • Security • DDL • DML • Privileged Users Events • Privileged Users • Sensitive Columns • Before-After Data auditing
DISA 2012 Instance SQL2-00-012400, SQL2-00-009700, SQL2-00-011800, SQL2-00-011900, SQL2-00-011400, SQL2-00-012000, SQL2-00-012100, SQL2-00-012200, SQL2-00-012300, SQL2-00-014700, SQL2-00-002300 **DISA 2014 Instance**	SQL Server must include organization-defined additional, more detailed information in the audit records for audit events identified by type, location or subject. Audit record content which may be necessary to satisfy the requirement of this control includes: time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, file names involved, and access control or flow control rules revoked. All use of privileged accounts must be audited. SQL Server must produce audit records containing sufficient information to establish what type of events occurred. SQL Server must produce audit records containing sufficient information to establish when (date and time) the events occurred. SQL Server must generate audit records for the DoD-selected list of auditable events. SQL Server must produce audit records containing sufficient information to establish where the events occurred. SQL Server must produce audit records containing sufficient information to establish the sources (origins) of events. SQL Server must produce audit records containing sufficient information to establish the outcome (success or failure) of events. SQL Server must produce audit records containing sufficient information to establish the identity of any user /subject associated with the event. SQL Server must support the employment of automated mechanisms supporting the auditing of the enforcement actions. SQL Server must enforce access control policies to restrict Alter server state permissions to only authorized roles. SQL Server must generate Trace or audit records when unsuccessful logins or connection attempts occur. SQL Server must generate Trace or audit records when logoffs or disconnections occur. SQL Server must generate Trace or audit records when successful logons or connections occur. SQL Server must generate Trace or audit records when concurrent logins/connections by the same user from different workstations occur. SQL Server must produce Trace or audit records containing sufficient information to establish when the events occurred. SQL Server must produce Trace or audit records of its enforcement of access restrictions associated with changes to the configuration of the DBMS or database.	Server Events: • Logins • Logouts • Failed Logins • Security changes • Privileged Users activity • User defined events • Privileged Users Database Events: • None

SQL4-00-011900, SQL4-00-012000, SQL4-00-012100, SQL4-00-012200, SQL4-00-012300, SQL4-00-037600, SQL4-00-037900, SQL4-00-037500, SQL4-00-037600, SQL4-00-037900, SQL4-00-038000, SQL4-00-011200, SQL4-00-036200, SQL4-00-036300, SQL4-00-038100, SQL4-00-034000		

DISA 2014 0	If SQL Server authentication, using passwords, is employed, SQL Server must enforce the DoD standards for password lifetime.	Server Events: - Security changes Database Events: - Security

FERPA Compliance

Section	Summary	Associated Audit Events and Features
99.2	**What is the purpose of these regulations?** The purpose of this part is to set out requirements for the protection of privacy of parents and students under section 444 of the General Education Provisions Act, as amended.	Server Events: - Successful and Failed Logins - Security changes Database Events: - Security changes
99.31 (a)(1)	**School officials** Institutions that allow "school officials, including teachers, within the agency or institution" to have access to students' education records, without consent, must first make a determination that the official has "legitimate educational interests" in the information. The list of officials must be included in the annual FERPA notification.	Server Events: - Successful and Failed Logins - Security changes - Privileged Users activity Database Events: - SELECT statements - Security changes - Sensitive Columns

99.31 (a)(1) (ii)	**Controlling access to education records by school** Institutions are now required to use "reasonable methods" to ensure that instructors and other school officials (including outside service providers) obtain access to only those education records (paper or electronic) in which they have legitimate educational interests. Institutions are encouraged to restrict or track access to education records to ensure that they remain in compliance with this requirement. The higher the risk, the more stringent the protections should be (e.g., SSNs should be closely guarded).	Server Events: • Successful and Failed Logins • Security changes • Privileged Users activity Database Events: • DDL • DML • SELECT statements • Sensitive Columns • Before-After Data auditing
99.31 (a)(2)	**Student's new school** An institution retains the authority to disclose and transfer education records to a student's new school even after the student has enrolled and such authority continues into the future so long as the disclosure is for purposes related to the student's enrollment/transfer. After admission, the American Disabilities Act (ADA) does not prohibit institutions from obtaining information concerning a current student with disabilities from any school previously attended by the student in connection with an emergency and if necessary to protect the health or safety of a student or other persons under FERPA. A student's previous school may supplement, update, or correct any records it sent during the student's application or transfer period and may identify any falsified or fraudulent records and/or explain the meaning of any records disclosed previously to the new school.	Server Events: • Successful and Failed Logins • Security changes • Privileged Users activity Database Events: • Security changes • DML • SELECT statements • Sensitive Columns • Before-After Data auditing

99.32 (a)(1)	**What record keeping requirements exist concerning requests and disclosures?** An educational agency or institution must maintain a record of each request for access to and each disclosure of personally identifiable information from the education records of each student, as well as the names of State and local educational authorities and Federal officials and agencies listed in § 99.31(a)(3) that may make further disclosures of personally identifiable information from the student's education records without consent under § 99.33 (b)(2). The agency or institution shall maintain the record with the education records of the student as long as the records are maintained.	Server Events: • Successful and Failed Logins • Security changes • Privileged Users activity Database Events: • Security changes • DML • SELECT statements • Sensitive Columns • SELECT statements
99.35 (a)(1)(2), (b)(1)	**What conditions apply to disclosure of information for Federal or State program purposes?** Authorized representatives of the officials or agencies headed by officials listed in 99.31(a)(3) may have access to education records in connection with an audit or evaluation of Federal or State supported education programs, or for the enforcement of or compliance with Federal legal requirements that relate to those programs. Authority for an agency or officially listed in § 99.31(a)(3) to conduct an audit, evaluation, or compliance or enforcement activity is not conferred by the Act or this part and must be established under other Federal, State, or local authority. Information that is collected under paragraph (a) of this section must: • Be protected in a manner that does not permit personal identification of individuals by anyone other than the officials or agencies headed by officials referred to in paragraph (a) of this section, except that those officials and agencies may make further disclosures of personally identifiable information from education records on behalf of the educational agency or institution in accordance with the requirements of 99.33(b).	Server Events: • Successful and Failed Logins • Security changes • Privileged Users activity Database Events: • Security changes • DML • DDL • Sensitive Columns • SELECT statements

GDPR Compliance

Section	Summary	Associated Audit Events and Features
Article 5	**Principles relating to processing of personal data** 1. Personal data shall be: a. processed lawfully, fairly and in a transparent manner in relation to the data subject (´lawfulness, fairness and transparency´); b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (´purpose limitation´); c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (´data minimisation´); d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (´accuracy´); e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (´storage limitation´); f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (´integrity and confidentiality´). 2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (´accountability´).	Server Events: - Privileged User - DDL - Privileged User - DML Database Events: - Privileged User - DDL - Privileged User - DML
Article 13 (1,e)	**Information to be provided where personal data are collected from the data subject** 1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information: e. the recipients or categories of recipients of the personal data, if any;	Server Events: - None Database Events: - Sensitive Column Auditing - Before-After Data
Article 24	**Responsibility of the controller** 1. [1]Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. [2]Those measures shall be reviewed and updated where necessary. 2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller. 3. Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller.	Server Events: - Logins - Failed Logins Database Events: - None

Article 25(2)	**Data protection by design and by default** 2. [1]The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. [2]That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. [3]In particular, such measures shall ensure that by default personal data are not made accessible without the individual´s intervention to an indefinite number of natural persons.	Server Events: • Logins Database Events: • Sensitive Column Auditing • Before-After Data • Privileged Logins
Article 30 (1)	**Records of processing activities** 1. [1]Each controller and, where applicable, the controller´s representative, shall maintain a record of processing activities under its responsibility. [2]That record shall contain all of the following information: a. the name and contact details of the controller and, where applicable, the joint controller, the controller´s representative and the data protection officer; b. the purposes of the processing; c. a description of the categories of data subjects and of the categories of personal data; d. the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations; e. where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards; f. where possible, the envisaged time limits for erasure of the different categories of data; g. where possible, a general description of the technical and organisational security measures referred to in Article 32 (1).	Server Events: • None Database Events: • Sensitive Columns • Before-After Data Change
32(2)	**Security of processing** 1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: a. the pseudonymisation and encryption of personal data; b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident. d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. 2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. 3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article. 4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.	Server Events: • None Database Events: • Sensitive Column Auditing • Before-After Data

Article 33	**Notification of a personal data breach to the supervisory authority** 1. [1]In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. [2]Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay. 2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach. 3. The notification referred to in paragraph 1 shall at least: a. describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned; b. communicate the name and contact details of the data protection officer or other contact point where more information can be obtained; c. describe the likely consequences of the personal data breach; d. describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects. 4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay. 5. [1]The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. [2]That documentation shall enable the supervisory authority to verify compliance with this Article.	Server Events: - Logins - Failed Logins Database Events: - Privileged Users
Article 35(7)	**Data protection impact assessment** 7. The assessment shall contain at least: a. a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller; b. an assessment of the necessity and proportionality of the processing operations in relation to the purposes; c. an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and d. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.	Server Events: - None Database Events: - Sensitive Column Auditing
Recital 39	**Tasks of the data protection officer** 1. The data protection officer shall have at least the following tasks: a. to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions; b. to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits; c. to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35; d. to cooperate with the supervisory authority; e. to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter. 2. The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing,	Server Events: - None Database Events: - Sensitive Column Auditing - Before-After Data

HIPAA Compliance

Section	Summary	Associated Audit Events and Features

164.306 (a, 2)	**Security Standards** Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.	Server Events: • Failed Logins • Security Changes • DDL • Privileged Users activity Database Events: • DML • Sensitive Columns
164.308 (1, i)	**Security Management Process** Implement policies and procedures to prevent, detect, contain and correct security violations.	Server Events: • Failed Logins • Security Changes • DDL • Privileged Users activity Database Events: • None
164.308 (B)	**Risk Management** Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a).	Server Events: • Failed Logins • Security Changes • DDL • Privileged User activity Database Events: • None

164.308 (D)	**Information System Activity Review** Implement procedures to regularly review records of information system activity such as audit logs, access reports and security incident tracking reports.	Server Events: • Failed Logins • Security Changes • DDL • Privileged Users activity Database Events: • Security • DDL • Administrative activities • DML • Sensitive Columns
164.308 (3, C)	**Termination Procedures** Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a) (3) (ii) (B) of this section.	Server Events: • Security Changes Database Events: • Security
164.308 (5, C)	**Implementation Specifications** Log-in monitoring (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies.	Server Events: • Failed Logins Database Events: • None

164.312 (b)	**Technical Standard** **Audit controls**. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	Server Events: • Failed Logins • Security Changes • DDL • Administrative activities Database Events: • Security • DDL • Administrative activities • DML • Sensitive Columns
164.404 (a) (1) (2)	**Security and Privacy** **General rule**. A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach. **Breaches treated as discovered**. For purposes of paragraph (a)(1) of this section, §§ 164.406(a), and 164.408(a), a breach shall be treated as discovered by a covered entity as of the first day on which such breach is known to the covered entity, or, by exercising reasonable diligence would have been known to the covered entity. A covered entity shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the covered entity (determined in accordance with the federal common law of agency).	Server Events: • None Database Events: • Security • Sensitive Columns
164.404 (c) (1) (A), (B)	**Security and Privacy** (c) Implementation specifications: Content of notification (1) Elements. The notification required by (a) of this section shall include, to the extent possible: (A) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known; (B) A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information.	Server Events: • None Database Events: • Sensitive Columns
HITECH 13402 (a) (f), (1), (2)	**Notification In the Case of Breach** (a) In General. A covered entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information (as defined in subsection (h)(1)) shall, in the case of a breach of such information that is discovered by the covered entity, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, or disclosed as a result of such breach. (f) Content of Notification. Regardless of the method by which notice is provided to individuals under this section, notice of a breach shall include, to the extent possible, the following: (1) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known. (2) A description of the types of unsecured protected health information that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, or disability code).	Server Events: • None Database Events: • Sensitive Columns

NERC-CIP Compliance

Section	Summary	Associated Audit events and Features
CIP-007-6 4.1	Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: detected successful login attempts, detected failed access attempts and failed login attempts; and detected malicious code.	Server Events: • Logins • Logouts • Failed Logins • Security changes • User Defined Events • Privileged Users • Privileged Users events Database Events: • Security changes • DDL • DML • Sensitive Columns • Before-After Data change • Privileged Users

PCI DSS Compliance

Section	Summary	Associated Audit Events and Features
2.1	Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network.	Server Events: • Failed Logins • Security Changes • DDL • Administrative activities • Privileged Users • User defined events Database Events: • Security • DDL • Administrative activities • DML • SQL statements • Sensitive columns
2.2	Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.	
3.4	Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: • One-way hashes based on strong cryptography, (hash must be of the entire PAN) • Truncation (hashing cannot be used to replace the truncated segment of PAN) • Index tokens and pads (pads must be securely stored) • Strong cryptography with associated key-management processes and procedures.	

6.2	Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.	- Before-After data change - Privileged users
8	Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for his or her actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.	Server Events: - Failed Logins - Security Changes - DDL - Administrative activities - Privileged Users Database Events: - Security - DDL - Administrative activities - DML - SQL statements - Sensitive Columns
8.5.4	Immediately revoke access for any terminated users.	Server Events: - Security Changes - Administrative activities Database Events: - Security
10	Track and monitor all access to network resources and cardholder data-logging mechanisms and the ability to track user activities are critical. The presence of logs in all environments allows thorough tracking and analysis if something does go wrong. Determining the cause of a compromise is very difficult without system activity logs.	See subsections
10.1	Implement audit trails to link all access to system components to each individual user.	Server Events: - Failed Logins - Administrative activities - Privileged Users activity Database Events: - None
10.2	Implement automated audit trails for all system components to reconstruct the following events: - 10.2.1 All individual user accesses to cardholder data - 10.2.2 All actions taken by any individual with root or administrative privileges - 10.2.3 Access to all audit trails - 10.2.4 Invalid logical access attempts - 10.2.5 Use of identification and authentication mechanisms - 10.2.6 Initialization, stopping, or pausing of the audit logs - 10.2.7 Creation and deletions of system-level objects	Server Events: - Failed Logins - DDL Database Events: - DDL - DML - Sensitive Columns

10.3	Record at least the following audit trail entries for all system components for each event: • 10.3.1 User identification • 10.3.2 Type of event • 10.3.3 Date and time • 10.3.4 Success or failure indication • 10.3.5 Origination of event • 10.3.6 Identify or name of affected data, system component, or resource	Server Events: • Failed Logins • Privileged Users activity Database Events: • Security • DDL • DML • Sensitive Columns
10.5	Secure audit trails so they cannot be altered.	SQL Compliance Manager Repository
10.7	Retain audit trail history for at least one year, with a minimum of three months online availability.	Enable archive and groom to retain Repository data for a minimum of one year

SOX Compliance

Section	Summary	Associated Audit Events and Features

404	A statement of management's responsibility for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and management's assessment, as of the end of the company's most recent fiscal year of the effectiveness of the company's internal control structure and procedures for financial reporting, Section 404 requires the company's auditor to attest to, and report on management's assessment of the effectiveness of the company's internal controls and procedures for financial reporting in accordance with standards established by the Public Company Accounting Oversight Board. (Source: Securities and Exchange Commission.) **What does this mean from an Information Technology standpoint?** The key is the reliability of financial reporting. Financial information resides in the database and it is the responsibility of IT to ensure the right personnel have access to that data at the right time. Any changes to the permissions must be tracked. Additionally, all access to that data (select, insert, update, and delete operations, plus before and after changes) must be audited down to the actual user and stored. If the need arises to determine where an individual has violated the accuracy of the financial data, an audit trail of activity will help to prove that the user: - Accessed the data - Changed permissions - Changed the data	Server Events: - Logins - Logouts - Failed Logins - Security Changes - DDL - Privileged User activity Database Events: - Security changes - Administrative activities - DML - SQL statements - SELECT statements on all DB objects - SELECT statements on specific tables - Before-After Data auditing - Sensitive Columns - Alerting
404 CDC	Implement change data capture.	Server Events: - None Database Events: - Sensitive columns - Before-After data change

IDERA | **Products** | **Purchase** | **Support** | **Community** | **Resources** | **About Us** | **Legal**