****

**Specification**

**for**

**Audit Templates**

**Robert Wilkinson**

**06/26/12**

IderaLogo

Proprietary and Confidential to BBS Technologies, Inc.

**© 2009 BBS Technologies, Inc.; all rights reserved.**

# Revision history:

|  |  |  |
| --- | --- | --- |
| **When?** | **Who?** | **What?** |
| 06/27/2012 | Robert | First Draft |

# Table of Contents

1. Revision history: ii

2. Table of Contents iii

3. Requirements 1

3.1. Overview/Purpose 1

3.1.1. Related Customer Requests 1

3.2. Use Cases 1

3.3. Feature/Function Market Requirements 2

3.3.1. Required Functions 2

3.3.2. Non-Supported Functions 3

3.4. Open Questions 4

4. Functional Design 5

4.1. User Interfaces 5

4.2. Installation and Upgrade 9

4.3. Permissions and other Required Configuration 9

4.4. Licensing Issues 9

4.5. Dependencies 9

4.5.1. Dependencies on Idera Software 10

4.5.2. Third-Party Software Required on the Customer Machine 10

4.5.3. Third-Party Software Required Internally 10

5. Internal Design 10

5.1. Architecture 10

5.2. Installation Issues 11

5.3. Schedule 11

5.3.1. Work Breakdown and Sizings 11

5.3.2. Areas of Risk 11

6. Quality Assurance Considerations 11

6.1.1. Overview 11

7. Documentation Considerations 11

8. Bibliography 12

# Requirements

## Overview/Purpose

Many customers have requested the ability to setup auditing based on a regulation. They are giving a section of a regulation and told to comply with it. Not knowing how to do that, they have to call support. This feature will allow the user to configure database auditing based on a regulation.

### Related Customer Requests

9508 – FRQ: Audit Templates.

Lots of customers (too many to count) want an alert when an operational error occurs such as trace directory full or collection services lost contact with an agent.

9488 – Change Log should indicate that an import action took place.

11341 – HIPAA Template for Auditing

11340 – PCI Template for Auditing

## Use Cases

1. Users should receive alerts when something is wrong with the operation of SQL compliance.
2. Users should be able to view these operational alerts in the alerts view.
3. Users should be able to create and configure these alerts from the Alerts ribbon in the Administration view.
4. Users should receive an alert when the collection service loses contact with an agent.
5. Users should receive an alert when the collection service trace directory is greater than a certain percentage full.
6. Users should receive an alert when the monitored server’s repository database grows greater than a certain size.
7. Users should receive an alert when the sum of all event repository databases and archived event databases is greater than a certain size.
8. Users should receive an alert when an agent’s trace directory is greater than certain percentage full.
9. Users should receive an alert when an agent cannot communicate with a monitored instance.

## Feature/Function Market Requirements

### Required Functions

#### Audit Templates

This feature will allow the user to setup database auditing based on a regulation. Currently we will only support PCI and HIPAA.

To setup auditing, the user will selected “Apply Audit Template” from the Database summary tab on the ribbon or from the database node context menu and a wizard dialog will be displayed.

The wizard will be comprised of 4 pages (See Section 4.1):

1. Regulation – This will allow the user to select one or more regulations to apply to a database. This page will also contain descriptive text about each regulation. (See Section 4.1.1)
2. Sensitive Column Auditing – This page will allow the user to select specific tables from the database for Sensitive Column Auditing. This page will be identical to the Sensitive Column Auditing tab on the Database Properties dialog with the addion of some text that will talk about what sections of the regulation Sensitive Column Auditing applies to (if any). (See Section 4.1.2)
3. Before/After Data Auditing - This page will allow the user to select specific tables from the database for Before/After Data Auditing. This page will be identical to the Before/After Data Auditing tab on the Database Properties dialog with the addion of some text that will talk about what sections of the regulation Before/After Data Auditing applies to (if any). (See Section 4.1.3)
4. Summary – This page will be a summary of the selected options from the previous pages. There will also be a link or button that will display a Summary dialog that will be a matrix of the regulation sections and SQLcompliance manager event categories. (See Section 4.1.4)

Only certain sections of the regulations apply to SQLcompliance manager. Version one of this version will “enable” all applicable sections. There will not be a way for the user to “opt out” of one or more sections.

Once the wizard has been finished, the selected regulation will be displayed for each database in the Audited activity section of the Database Summary view. (See Section 4.1.5)

There will also be a new Report that will select a database and view the regulation that has been applied to it. The report will be almost identical to the Summary page of the wizard.

### Non-Supported Functions

1. The user will not be able to “opt out” of one or more of the applicable sections.

## Open Questions

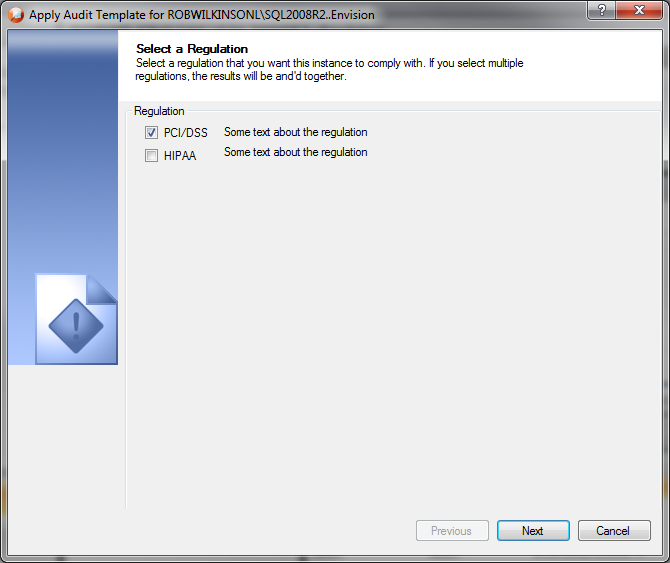
1. None

# Functional Design

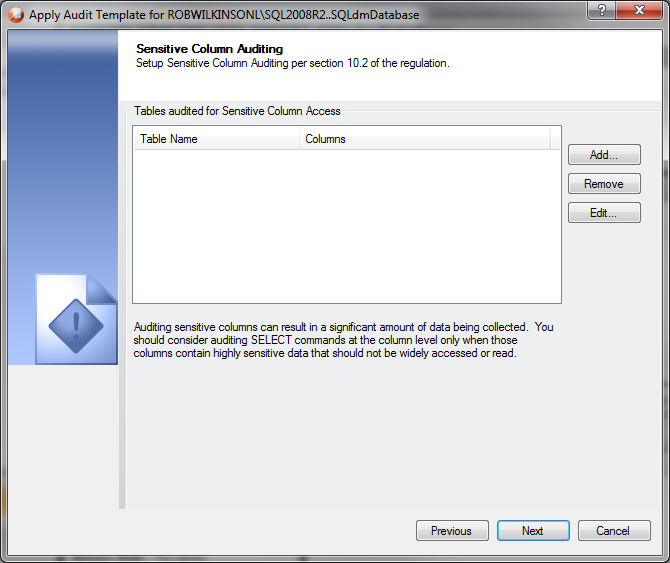
## User Interfaces

The wizard will be accessed 2 ways. A button on the database summary tab of the ribbon and as an option on the database context menu.

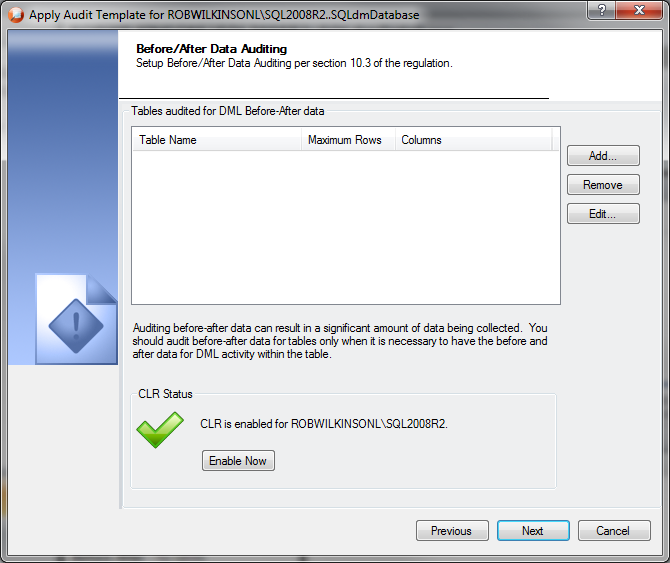
### Regulations



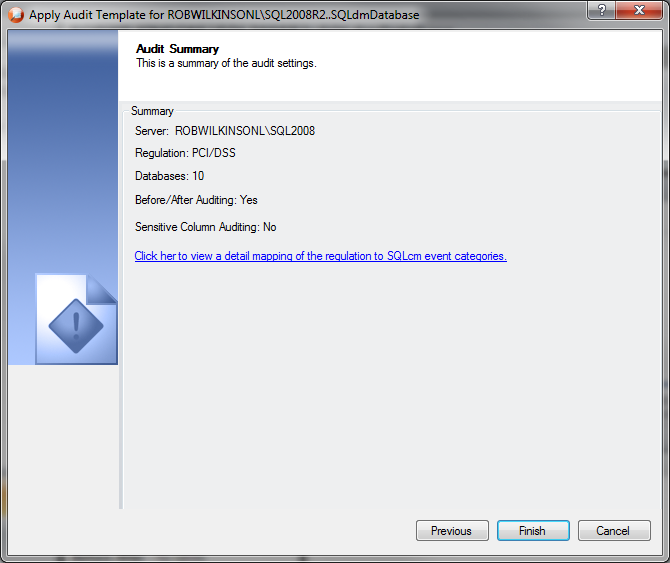
### Sensitive Column Auditing



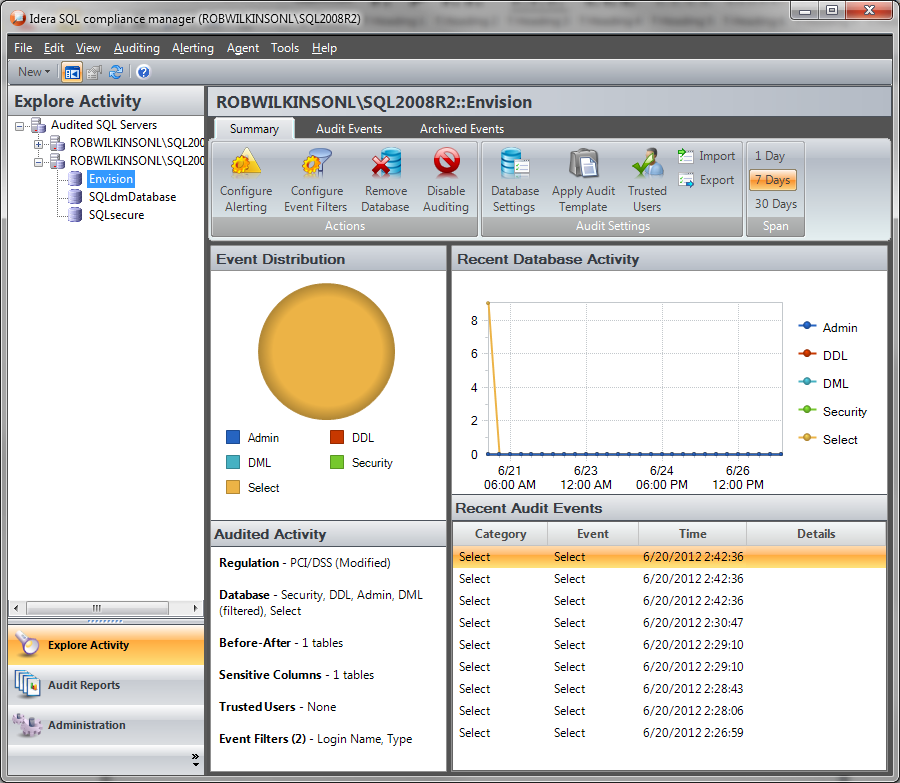
### Before/After Data Auditing



### Summary



### Audited Acitivity Summary



## Installation and Upgrade

None

## Permissions and other Required Configuration

The user must have modify rights to add alert rules. Otherwise, everything will be read only.

## Licensing Issues

None

## Dependencies

None

### Dependencies on Idera Software

None

### Third-Party Software Required on the Customer Machine

None

### Third-Party Software Required Internally

None

# Internal Design

## Architecture

An overview of the architecture behind this feature – how it works, components, communication between components etc

There will be two new tables added to the repository to store the regulation mapping.

1. Regulation

ID, Name, Description

1. RegMap

ID, Section, Section description, event Category

There will be a new column added to the in the Databases table to store what regulation has been applied to a database.

Regulation – Null = none, 0 = PCI, 1 = PCI modified, 2 = HIPAA, 3 = HIPAA modifed

## Installation Issues

None.

## Schedule

### Work Breakdown and Sizings

|  |  |  |
| --- | --- | --- |
| Component | Who | Sizing (Days) |
| Audit Templates Wizard – UI Only | Robert | 2 |
| Repository Changes – Insert Regulation data into new tables | Robert | 2 |
| Repository Changes – New tables and columns | Robert | 2 |
| Audit Template Wizard – Functionality | Robert | 2 |
| Template Summary Dialog | Robert | 2 |
| Report | Robert | 2 |
| Testing | Robert | 2 |
| **Total** |  | **14** |

### Areas of Risk

None

# Quality Assurance Considerations

### Overview

None

# Documentation Considerations

* None.

# Bibliography