

SOX Compliance

Visual Dolphin security compliance to
the Sarbanes-Oxley Act

About SOX and IT Security

Sarbanes-Oxley Act compliance has become a major course of action within organizations. Enacted in 2002, the law was a response to a number of major corporate and accounting scandals and it set new and enhanced security standards. Its intention is to close every possible security crack, mainly in financial and accounting data and the database and application layers. SOX also allows an outside audit and security analysis of any data manipulation.

It's been proven that most security problems come from within the organization. That said, it is essential to first implement internal security and to make sure the right people have access to the right data. SOX compliance and security best practices impose these three rules, also applied when it comes to securing the data:

Confidentiality-Integrity-Availability

- **Confidentiality** -- Protecting sensitive information from unauthorized disclosure or intelligible interception.
- **Integrity** -- Safeguarding the accuracy and completeness of information and software.
- **Availability** -- Ensuring that information solutions are available when required.

Visual Dolphin Development & Database Compliance

Development Compliance with SOX requirements

a. Password Policy Rules	i) Minimum Length – Expiry Date – Complexity – Last Usage Prohibited – Locking user after trying multiple unsuccessful logins. ii) Report: Visual Dolphin Password Change Report
b. Security Logs Saved in Database	i) Log tables should be created to hold information such as change in access for a user, change in prices for a customer, and Client/Supplier Details changes. ii) Reports: <ol style="list-style-type: none"> a. Visual Dolphin Log Security Customers Report b. Visual Dolphin Log Security Vendors Report c. Visual Dolphin Log Security for Charts of Accounts d. Visual Dolphin Log Security Price Lists Report e. Visual Dolphin Log Security User Information Report f. Visual Dolphin Log Security User Group Report g. Visual Dolphin Log Security User Access Level Report

c. Security Groups and Users	<ul style="list-style-type: none"> i) The ability to report the groups available in the database with their respective privileges. ii) The ability to report the users and to which groups they belong. iii) The ability to report the Media Cycle Actions enabled as security steps. iv) Reports: <ul style="list-style-type: none"> a. List of Users Group Membership, arranged by Groups b. List of Visual Dolphin Actions c. List of Visual Dolphin Groups d. List of Visual Dolphin Access Level
d. Visual Dolphin Database Health	<ul style="list-style-type: none"> i) The ability to report the groups available in the database with their respective privileges. ii) Database Health Check – Diagnostic iii) Report: Visual Dolphin Database Health Check

Processes Involving Visual Dolphin

a. User Validation	
b. Control Report	Visual Dolphin Month to Month Access Changes by Group by User.

Software Development Life Cycle

a. Release Management	<ul style="list-style-type: none"> i) Releases are documented with changes description and explanation. ii) Releases are tested. A proof is handed to the client as a printed document stamped by Software Design. The document includes: <ul style="list-style-type: none"> a. All Reports b. All Screens testing where a change took place iii) Releases are installed on the testing server of Visual Dolphin for a maximum of 1 month before rolling it to the client production server, in case of suitability and stability of the system.
-----------------------	--



Lebanon	Phone	961-1-399855
	Fax	961-1-380420
	PO.Box	166607 – 1100 2140 Ashrafieh Beirut – Lebanon
United Arab Emirates	Phone	971-4-3383318
	Fax	971-4-3383319
	PO.Box	35046 Al Romoul Dubai – U.A.E.
Saudi Arabia		
	Riyadh	Phone 966-1-4730784 Fax 966-1-4730784
	Jeddah	Phone 966-2-6608824 Fax 966-2-6603835
	PO.Box	5586 Riyadh 11432 - Kingdom Of Saudi Arabia
	Email	sdcg@softwaredesign.com.lb
	Website:	http://www.sd-lb.com