How Security and Audit Trails are Embedded Within VCIS? The Strategic Value Generation Behind it

In an era marked by the escalating diversity and dispersion of security threats, governments and corporate entities are navigating a landscape that demands heightened resilience and risk containment. This paradigm shift is palpable in daily headlines, reflecting a new mentality adopted by governments and corporate security teams alike. In response to this evolving threat landscape, VCIS (VALOORES Compliance & Information Security) emerges as a pivotal solution, offering a robust security framework coupled with an advanced Audit Trail system.

From dynamic data processes to business process management, user management, and robust security features, VCIS proves to be a versatile solution for organizations navigating the complexities of modern security challenges.

Table of Contents

1. How is Security Translated in VCIS?

With the increasing diversity and dispersion of threats, governments are adopting a new mentality towards resilience and risk. This is evident from the daily headlines that we see. In parallel, corporate security teams have also shifted their focus towards strengthening resilience and containing risk. In this context, VCIS Security and Audit Trail presents a promising solution.

By leveraging machine learning, VCIS has the potential to process vast amounts of data, thereby enhancing security. For instance, VCIS can analyze millions of pictures and videos to detect anomalies like overcrowding or fires. As a result, computers can learn to recognize and respond to such anomalies in security data and video in real-time, making VCIS a valuable tool for corporate security teams.

2. Dynamic Data Integration: Why and How to use it?

Purpose

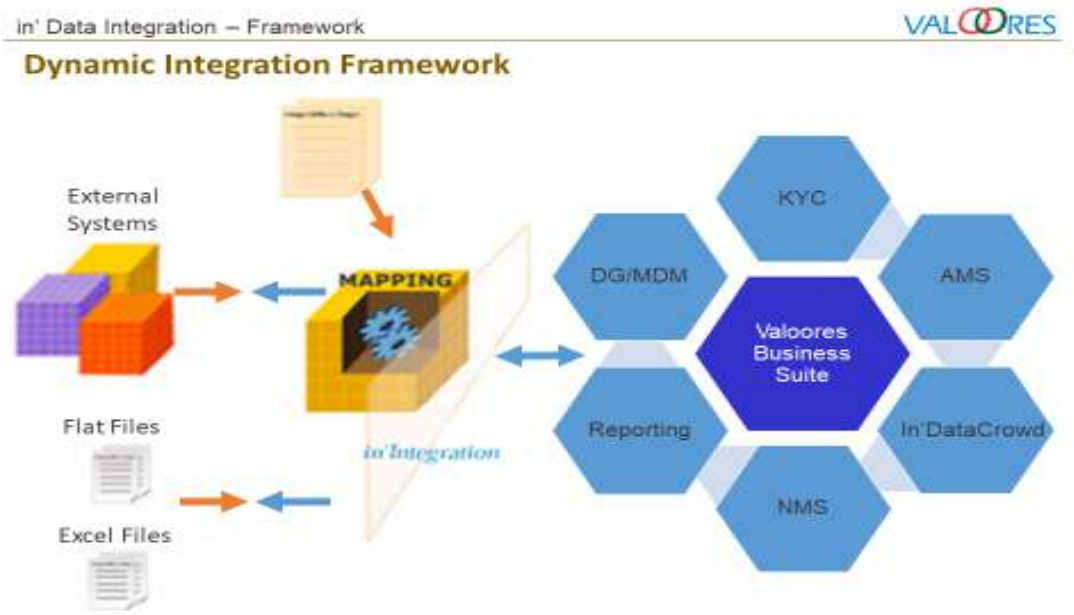
Dynamic Data Integration and Synchronization, Inbound and Outbound Flow, Follow-up on data integration logs.

Data Integration

Import/Export Data, Flat and Excel files, formulas and data transformation, manual or automatic execution, Bulk Data Integration using SQL Loader, Staging table configuration.

Logging capability

Logging the Data Load Execution and logging the Interfaces Inventory Execution.



3. Data Integration Process

Setup

The initial stage of data integration includes three key actions: creating a flat or Excel file (with optional headers), setting up staging tables to process data, and selecting the creation type, either import or export.

Data mapping

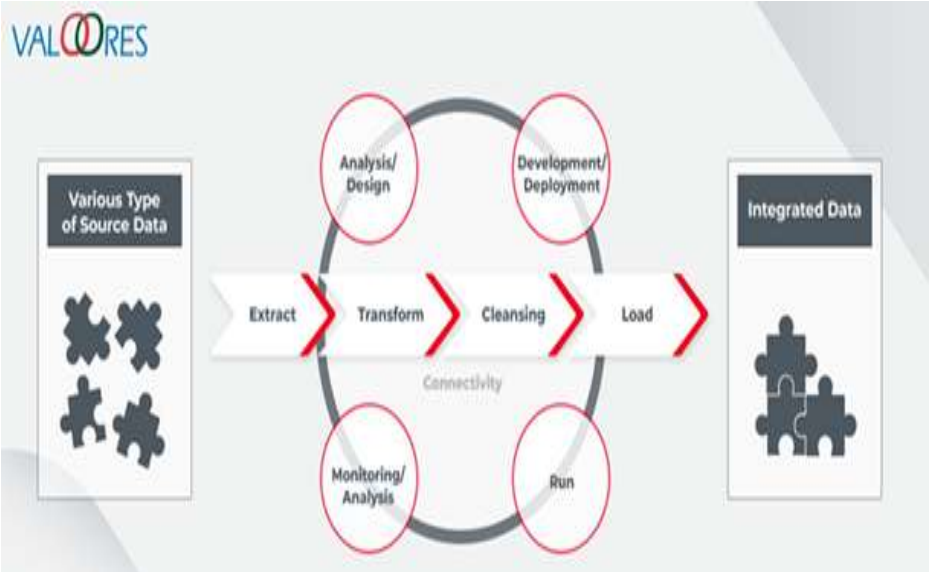
There are two main procedures involved in this process. The first is visual direct mapping, which involves mapping data directly using visual aids. The second is data mapping defaulting, which can be done through two methods: defaulting to the default value or cross-referencing based on data matching.

Simulation

Simulation tests data loading into the Database and checks business rules.

Logs

Logs detect the logging capability, bad files and log files content, log viewer and search.



4. Dynamic Business Process Management: Why & How to Use it?

Purpose

- Automation of Business Process Management
- Creation of Personalized scenarios
- Presenting a Large choice of triggering events and actions
- Services coverage.
- Business process flow coverage

Process Status can be

- Active
- Inactive
- Pending Approval
- Escalated
- Closed justified, etc…

Detailed Actions

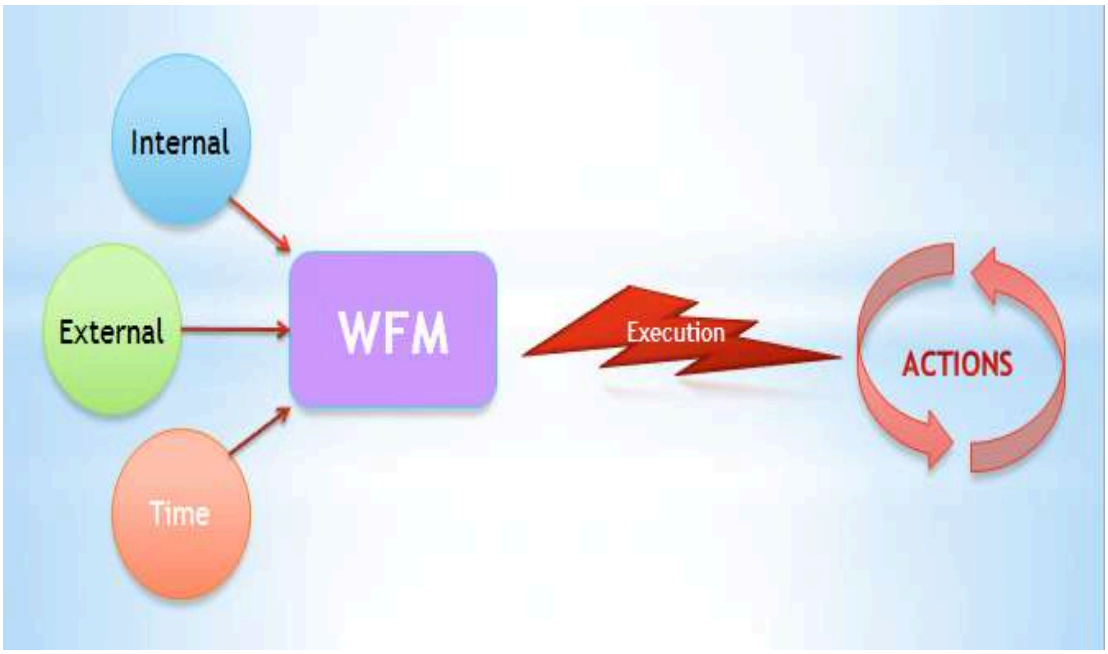
Activities Definition and applying business processes in an organization.

5. Triggering Events: There are three main types of triggering events

Internal: Application field/table modifications (Add/Modify/Delete)

External: Incoming events from external applications/ Third Party provider.

Time: Scheduled Events



6. Business Process Actions

Sending internal alerts
Applicative emails such as messages.

Sending email messages
Internal to all suite users.
External to suppliers, contacts, third party systems.
Dynamic based on Reporting by selecting a recipients list.

Executing operating system commands
Backups, file copies, file moving and shell/batch script execution.

Executing stored procedure
Applicative emails such as messages.

Generating XML files
Based on Integration by simply selecting prepared mapping scenarios.

Calling a web service
Based on in'Integration by simply selecting prepared mapping scenarios.

Sending SMS phone messages
For instant messaging purposes..

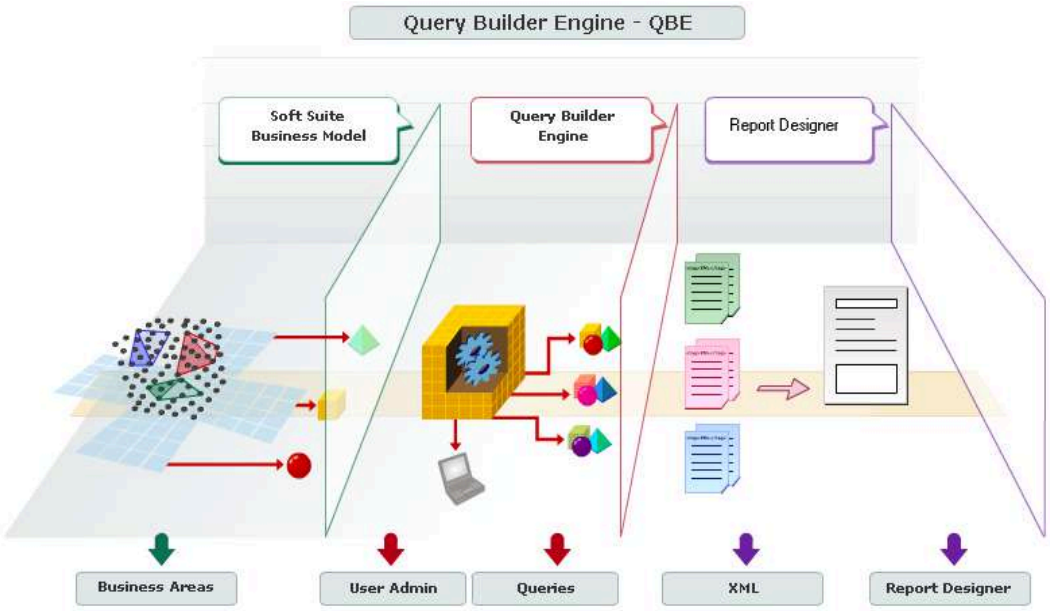
7. Designing Reports and Extracting data

Purpose

- Simple Access to all Services' Data
- Inessential to have a technical profile
- Use of Business Language
- Use of Business Model
- Build queries and reports
- Multi-formats execution

Detailed Actions

- Business Model: Business view of the Database following application logic, organized in a Business point of view with Business Areas
- Query Builder Engine: Retrieves information from business areas, is based on business model, uses formulas and filters, queries are exportable
- Report Designer: created reports based on queries, chart builder, all design functionalities, reports exportable.



8. Report Generation

- Ability to generate the report from in'Reporting
- Ability to generate the report from an application
- Ability to receive the report by an email, in a task, or in a Dashboard alert.

9. Users Management and Actions Follow Up

Purpose

- Management of users and their access rights
- Follow up on users' logs or actions
- Changing the application's configurations without technical intervention
- Management of all VALOORES applications parametrization

Managing users

By linking each user to its specific role(s). The role consists of different profiles providing access rights to different applications.

Detailed Actions

- User Logs: following up the logs by application or by menu, and by login date
- User Access Rights: inheriting the profile access rights to all sub-menus, defining exceptions by user if needed, giving access rights from the highest level of application to the lowest (fields or buttons).
- Application parameters: fields and date formats configuration, password settings configuration, server configuration, etc.

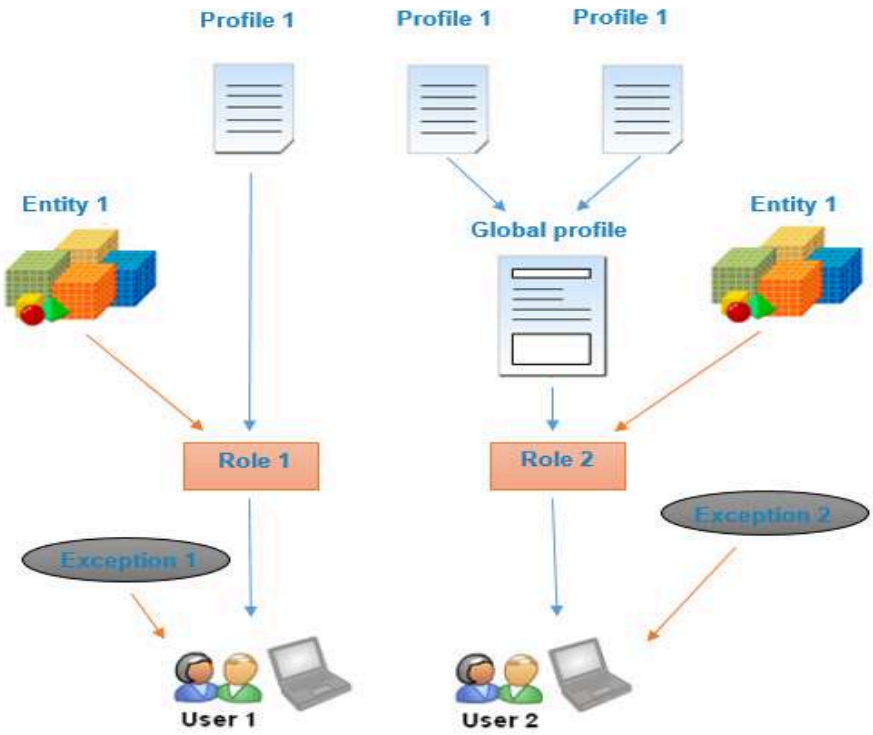
10. VCIS in Security

The cybersecurity sector is rapidly expanding due to the continuous advancement of cyber attackers' techniques and tactics. They can compromise a system within seconds, and their attacks sometimes remain undetected for months. One of the main challenges in detecting such attacks is that they happen quickly, and the indicators can be dispersed across various data sources, such as network servers, endpoints, and applications.

The VCIS security system provides organizations with the necessary visibility to detect complex attack techniques such as compromised credentials, lateral movement, and data exfiltration. Unlike traditional security tools, it facilitates the early detection of attackers by analyzing user account activities for insider threat behaviors.
VALOORES Security manages user profiles, roles, and access authentication at all precautionary levels, ranging from normal non-private privileges to highly safe measures.
In addition, VCIS security assists organizations in complying with

government regulations. It monitors access, authentication, and user behavior, helping with insider threat detection, and collects log data for auditing.

Security is a vital component of the VCIS platform, which is highly embedded within the application and translated in terms of restrictions, authentications, and precautionary measures.
Talking about restrictions, VCIS offers governments the ability to choose an area on the map and mark it as a restricted area. By adding this feature, users will not be able to conduct any type of report to display hits in the restricted area. For example, VIP, Royal, Normal, Private, Political Residence, Sport Stadium, Borders, and Transportations are different types of restricted areas. User management provides control over different data sets such as telecommunications data, private data, internal data, SDK, and geospatial data. Therefore, the engines and the simulation outputs will be executed based on the specific data type linked to the users.



11. Audit trail

In today's digital world, audits are directly linked to software, IT infrastructure, and actions on data in electronic format. Therefore, all information and evidence must be ensured by secure electronic means. Audit trails are essential in maintaining a record of system activity by both system and application processes and user activities on systems and applications. When used in conjunction with appropriate tools and procedures, audit trails can help detect security violations, performance problems, and application flaws. An audit trail is a sequence of records of events related to an operating system, application, or user activities. A computer system may have several audit trails, each dedicated to a specific type of activity.

Auditing involves the review and analysis of management, operational, and technical controls. Auditors can obtain valuable information about activity on a system from the audit trail. Audit trails improve the system's auditability and increase the likelihood of detecting unauthorized activities. Therefore, they are crucial for businesses that are striving to go digital and must ensure the security and integrity of their electronic data.

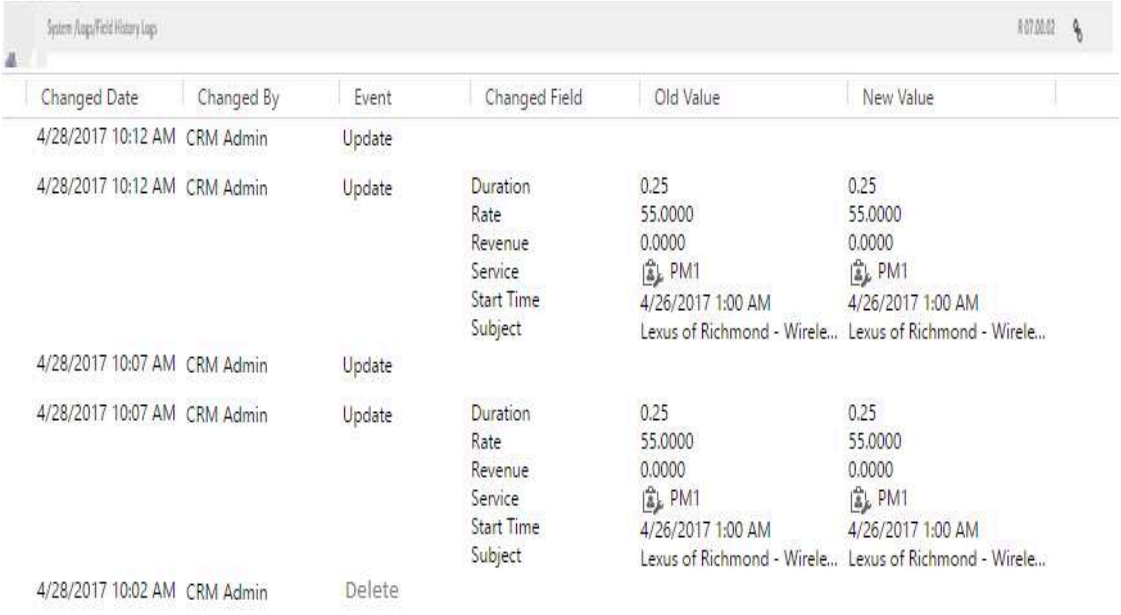
12. Audit trail within VCIS

VALOORES Audit Trail is a comprehensive register of every action, event, or activity executed by a user or system with your data. It covers various activities, such as creation, modification, and deletion of records, as well as a sequence of automated system actions (Syslog). However, the daily volume of audit logs can vary from hundreds to hundreds of thousands, making it challenging to track manually. Therefore, an automated tracking solution is necessary to ensure comprehensive coverage.

VALOORES Audit Trail enables automated tracking of all user actions, from logging in to accessing, performing any activity, and updating. This provides complete visibility into user activity, which is essential for identifying security violations, performance problems, and flaws in applications. The ability to track all actions, events, or activities related to data is crucial for businesses that need to ensure the security and integrity of their electronic data.

The audit trail is crucial for any solution because it can give benefits from:

- Compliance: Audit trail is a requirement.
- Internal fraud: Managing multiple systems or users accessing your data can be challenging, regardless of the scale of the operation. Keeping track of all activities can be time-consuming, resource-intensive, and can pose hidden risks if not done correctly. Therefore, it is essential to have a solution that enables efficient and automated tracking of all user actions and system activities. This allows businesses to monitor and analyze system activity, detect anomalies or unauthorized access, and ensure the security and integrity of their electronic data.
- Data breach: As time goes by, cybercriminals are becoming increasingly active and inventive. When working with personal data, which is highly sensitive, the risk of a data breach is almost 30%. This is a significant risk that cannot be ignored.



Changed Date	Changed By	Event	Changed Field	Old Value	New Value
4/28/2017 10:12 AM	CRM Admin	Update			
4/28/2017 10:12 AM	CRM Admin	Update	Duration	0.25	0.25
			Rate	55.0000	55.0000
			Revenue	0.0000	0.0000
			Service	PM1	PM1
			Start Time	4/26/2017 1:00 AM	4/26/2017 1:00 AM
			Subject	Lexus of Richmond - Wirele...	Lexus of Richmond - Wirele...
4/28/2017 10:07 AM	CRM Admin	Update			
4/28/2017 10:07 AM	CRM Admin	Update	Duration	0.25	0.25
			Rate	55.0000	55.0000
			Revenue	0.0000	0.0000
			Service	PM1	PM1
			Start Time	4/26/2017 1:00 AM	4/26/2017 1:00 AM
			Subject	Lexus of Richmond - Wirele...	Lexus of Richmond - Wirele...
4/28/2017 10:02 AM	CRM Admin	Delete			