

WORKFLOW MANAGEMENT

Overview

The Swordfish Workflow Management functionality of the SWORDFISH platform smoothly connects all major elements of Information Security Management, from framework establishment and maintenance to continuous monitoring and reviewing.

Using this powerful workflow engine clients can develop, define and streamline security procedures. SWORDFISH allows the allocation of tasks to security roles as well as end-users, and defines deadlines, priorities and escalation paths, based on corporate security requirements and regulations.

Dynamic Workflow Engine

An embedded, sophisticated and powerful workflow engine can enforce security policies through automated and streamlined procedures that can be developed using the workflow builder embedded functionality.

A step by step approach within a user friendly interface utilizes self-guided features such as readily available drop down menus, check boxes and pre-configured action lists. All necessary workflow information regarding ownership rights, editing rights, involved procedure roles and related artifacts can also be entered in relevant Tabs effortlessly by users. The Workflow engine also offers the possibility of developing complex Workflows with inner loops and Sub-Processes.

The workflow development process is structured upon a simple and solid 5-step concept, allowing users with no extensive technical skills and knowledge to design workflows.

Workflow Automation

Workflow steps are automatically assigned based on User roles or relative position in the Org. Structure. **Workflow steps can be initiated manually on CISO Portal or can be timer-initiated.** Also, Workflow steps can automatically be escalated after a specific time period.



**Web Based
and Mobile
Friendly**

Manage your workflows using a standard web browser to connect to the platform. Internet Explorer, Mozilla Firefox, Google Chrome, Opera and Safari browsers are all supported. **Responsive by design** to support mobile devices, tablets and Smartphones.

Workflow Management

- Enforce policies through automated and streamlined procedures
- Assign tasks to security roles as well as end-users, define deadlines and escalation paths, based on corporate security requirements and regulations.
- Workflow steps are automatically assigned based on User roles or relative position in the Org. Structure.
- Workflow steps can be initiated manually on CISO Portal or can be timer-initiated.

Workflow Builder

- Develop, define and streamline security procedures.
- Design workflows via a step by step approach within a user-friendly interface utilizing self-guided features such as readily

available drop-down menus, check boxes and pre-configured action lists.

- Each workflow can be tested before deployed to production, in order for the workflow designer to verify correct execution according to the business requirements.

Dashboards and Reporting

- Generate complete and detailed reports for senior management & regulators to demonstrate compliance.
- An integrated logging and notification system, provides detailed activity records that can be reviewed and audited on a regular or ad-hoc basis.
- Notifications are designed and triggered according to corporate security procedures.
- Reports can be exported and kept in file for reference.

Benefits

1. Interoperability

Integrate with corporate portals, Microsoft Sharepoint, document management systems

How It Works

SWORDFISH open architecture allows it to integrate with corporate portals like Microsoft SharePoint and document management systems like LifeRay. Organizations can utilize SWORDFISH API in order to integrate workflows with their corporate intranet portals, achieving a more streamlined experience for their users. This way resistance to change is minimal and it is assured that security processes will be followed across the organization.

3-Tier Architecture and technical standards

Swordfish Platform is a Web based application following a typical 3 tier architecture. Users are able to access, modify, update and interact with already imported data – information via a Graphical User Interface (Presentation tier). User Requests and actions are handled and processed through a Web application server (Application tier) before any Data is stored, retrieved or altered in a Database server (Data tier) Swordfish is implemented using ASP.NET and IIS as the server platform. The back-end database storage is supported by MongoDB.



Benefits

Integrate with Third Party Workflow engines

How It Works

SWORDFISH Workflows can be customized in order to drive or be driven by external workflow mechanisms. As a native .NET application, Swordfish can integrate with Microsoft BizTalk Server as well as with other BPEL engines through Web Services.

Integration with Third Party Ticketing Systems

Today organizations use many different ticketing systems like JIRA, Bugzilla, Redmine, Git etc., for the many different business matters that also affect security. For example, customer support may use JIRA to log customer requests while Development teams may use Git to log bug fixes and enhancements made to software products. SWORDFISH can be integrated with those third-party ticketing systems in order to bring security in every business context and update relevant information like risks, non-compliance issues, vulnerabilities and assets when required.

2. Information Security

Auditing and Logging

The Swordfish Platform offers embedded full scale auditing & logging functionality regarding all user actions and activities and has the ability to produce several relevant Reports. Specifically, out-of-the box reports relevant to users actions indicatively include but are not limited to:

- **Users Activities**
- **Application Usage Status**
- **Users workflow actions,**
- **Procedures status,**
- **On time completed actions,**
- **Pending tasks**
- **Deadlines for procedures' steps,**

Reports can be produced in several types of formats such as:

- **Pdf / • Xls / • Image /**
- **Dynamic Workflow Engine Csv**

Apart from reporting engine, Swordfish Platform extensive logging functionality also provides to authorized users the following information regarding application usage:

- **User IP**
- **Date & Time of user login and logout**
- **Session ID**

Reporting

The reporting module/engine allows clients Information Security department to produce out-of-the-box as well as custom reports. Given, the entire contents and configuration of the Swordfish platform are stored in the database layer, virtually any custom report pertaining to the content of the Swordfish Platform can also be produced.

Access Control

Swordfish uses a Role-based access control system in order to control access to modules and documents based on the classification scheme of the organizations. Besides the classic login screen, Swordfish can be integrated with Active Directory in order to enable single-sign-on functionality (if installed internally in the organization).



Benefits

How It Works

Need to know Principle

Access to menus, views, reports, local information download and in general layers of information is implemented according to the "need-to-know" principle where users are offered the minimum possible information in order to perform their duties.

3. Information Security

Workflow Design

The workflow development process is structured upon a simple and solid 5-step concept allowing users with no extensive technical skills and knowledge to design workflows via a step by step approach within a user friendly interface (the workflow builder) utilizing self-guided features such as readily available drop down menus, tick boxes and pre-configured action lists.

Testing Functionality

Each workflow can be tested before deployed to production, in order for the workflow designer to verify correct execution according to the business requirements.

Dynamic Workflow Engine

An embedded, sophisticated and powerful workflow engine can enforce security policies through automated and streamlined procedures that can be developed using the workflow builder embedded functionality. All necessary procedure information regarding ownership rights, editing rights, involved procedure roles and related artifacts can also be entered in relevant Tabs effortlessly by users. The Workflow engine also offers the possibility of developing complex Workflows with inner loops and Sub-Procedures.

Dynamic Forking

Workflow forking is supported, in order to escalate the appropriate tasks to asset owners with dynamic allocation of resources based on user's input during the execution of the flow.



Obrela Security Industries provides security analytics and risk management services to identify, analyse, predict and prevent highly sophisticated security threats in real time.

Tel: +44 (0) 203 397 8723 / info@obrela.com
24th Floor, One Canada Square, Canary Wharf,
E14 5AB, London, United Kingdom

obrela.com

