Swordfish
Security Technology

COMPLIANCE MANAGEMENT

Overview

The implementation and monitoring of an Information Security Framework constitutes not only a business need but also a regulatory obligation for many organizations. Identifying such needs in the market, SWORDFISH assists businesses in demonstrating the compliance of their entire organization against internal security policies, international standards and government regulations, through audit questionnaires and procedure enforcement statistics.

Our solution is able to compile real-time and ad-hoc reports for senior management, auditors and regulators.

Map Standards to your Framework

By leveraging the SWORDFISH platform capabilities, client organizations will be able to map policies and standards to their corporate objectives and regulative sources, such PCI, ISO/IEC, COBIT, HIPAA, SOX and privacy protection acts.

Objectives and sources can be added over time as your business evolves and new regulations, best practices and internal requirements emerge.

Monitor and Enforce compliance

Enforcement of an IS Framework and monitoring the compliance level of an organization is typically a resource intensive task especially in large corporate environments. In this regard the ISF enforcement, facilitation and monitoring are built-in platform attributes. Monitoring and evaluation of the ISF enforcement level is performed centrally via the web based console. Via the Compliance module, client security organizations can have a clear view of the Information Security processes and related ISF components enforcement and execution current status. Monitoring and evaluation of enforcement level and status of ISF active procedures can be performed through multiple panels, offering also graphical representation of the organization's overall compliance status, pending tasks that need to be a ddressed and areas of non-compliance.

OBRELA
SECURITY INDUSTRIES

Collaboration

The involved parties are notified online via the embedded **notification subsystem** as well as via e-mail. Furthermore, a Calendar Sub-System provides to each individual involved user the possibility to have a **Graphical representation** of their procedures tasks, milestones, deadlines and actions status in dynamic calendars. Nevertheless, the workflows can provide notification alerts via the notification sub-system in order to provide 24x7 monitoring and alert function regarding workflow milestones, bottlenecks or critical paths. Notifications are customizable and typically related to assigned tasks, escalation requests, new release of ISF documents and in general any pending actions.

Assesements

- Create assessment questionnaires using the built-in tool - "Questionnaire Builder"- & assess compliance against regulatory frameworks, international standards and security best practices.
- Review assessment questionnaires by automatically assigning sections of each questionnaire to appropriate personnel for review.

Compliance Planning

- Organize and plan mitigation actions for each exposure gap that has been identified.
- Follow up mitigation actions and enforce deadlines for each working package.

Reporting

- Generate complete and detailed reports for senior management & regulators to demonstrate compliance.
- Create Ad-hoc reports on the compliance status of your organization and 3rd party Vendors you may have assessed.
- Reports can be exported and kept in file for reference.

Benefits

How It Works

1. Compliance Assessment

Build Assessment Questionnaires based on applicable controls

Security Policies, controls and mandates can be easily imported in the Swordfish platform in the form of Compliance questionnaires, allowing clients to execute Compliance Assessments against the new requirements in order to easily identify areas of non-compliance and take appropriate ISF improvement actions.

Measure and report compliance to laws, regulations and internal policies

To demonstrate against Legal & Regulatory requirements, as previously described, Swordfish offers the capability to easily import Compliance questionnaires, virtually any International Standard, (ISO 27001, NIST, BSI, PCI/DSS etc.), enabling our clients to perform Compliance Assessments in order to identify non Compliance areas and take appropriate ISF improvement and enforcement actions.

Benchmark internal policies against ISO, PCI, NIST et.

Moreover, via the cross referencing and indexing functionality provided, our clients are able to perform Compliance Assessments for every individual standard in order to measure its compliance against it. ISF Documents can be cross-referenced, on a chapter, section and paragraph level with external documents such as International Standards (ISO 27001, NIST, etc,) and legal and regulatory bodies mandates in order to demonstrate compliance.

Benefits	How It Works
Provide a single repository of Compliance Related documentation	All compliance material is handled separately under the compliance module. Access rights can be applied both under user management and classification scheme. Assessment questionnaires and reports are also included.
Run assessments against all targeted groups	Compliance assessments can be run to targeted groups using "scoping" functionality that enables assessments to be executed based on roles, locations and areas of responsibility. addressing roles, geographical locations, business units, area of responsibility

2. Compliance Planning

Provide all non-compliance issues under a single compliance planning scheme.	Non-compliance issues can be categorized, assigned, scheduled and monitored via the Compliance module under a single compliance planning scheme that includes responsibility, schedule for implementation, ownerships etc.
Embedded ticketing system enables assignment of tasks to responsible entities	Non-compliance tasks can be assigned to individuals based on role management and responsibilities.
Tracking of Activities	Compliance tracking through the compliance module.

3. Vendor Assessments

Tailored to Vendor requirements in terms of frequency, content and context.

The process and the related content is completely tailored to the organization security policy and structure including but not limited to Role-Management Sub-System & Authentication Engine to tackle the multiple internal and external roles participating in the process and the challenges of the fine grained access levels required to offer security without hindering ease of use.

- **Content Management module to enable online Vendor Assessment questionnaires completion while the Questionnaire Builder subsystem allows for customized Assessment questionnaires to be addressed to different vendor groups or individual vendors.**
- **Document Management module to enable uploading of offline completed Vendor Assessment questionnaires and apply versioning.**
- **Workflow Engine to design and operate the Vendor Assessment Process**
- **Reporting Engine to offer statistical and compliance reports**
- **Notifications Engine to handle the intensive communication and messaging requirements of the Vendor Assessment process**
- **Calendar Sub-System to handle the intensive scheduling and Compliance Monitoring requirements of the Vendor Assessment process**

Assign applicable controls based on Vendor Criticality

Vendors are assessed based on Criticality both in terms of Frequency but also in terms of content and context.

Generate automatic reports

Vendor assessment reports are automatically generated following the vendor assessment cycle. The reports can be circulated to the appropriate people inside the organization in order to take further actions or raise risks related to vendor management.

Provide Web Based Interface for Assessments

Vendors can use the CISO portal to answer assessment questionnaires in an easy and intuitive way by using dynamic forms. Vendors are automatically notified by e-mail when an assessment tasks arrives in their CISO portal inbox and can escalate their tasks using a custom organizational scheme inside the main organization.

Run Assessment based on a Dynamic Workflow

Standard Vendor Assessment processes already exist as part of the SWORDFISH library. However, the organization can tailor the vendor assessment process according to it's specific needs. The processes can be published and made available for Vendors with a simple click.

Run Assessments on-line

There is no need to install anything on Vendor's systems: All Assessments are performed on-line via our user-friendly CISO-portal on desktop or mobile.

4. Reporting

Customized Reporting

Standard reporting for risk assessment exists including a standard set of dashboards to address corporate risk management views and maximum value to the board. Risks can be aggregated based on Business Unit, Geographical Location or Region, Area of Responsibility or group of systems etc. Reports can be customized as per client's requirements.

Global Risk Views and Dashboards

Vendor performance can be easily evaluated with the built-in dashboards that identify the risks related to each vendor per Asset, Business Unit or Business Service at global or regional level. Performance metrics can be extracted, supporting management in decision making and further enhance vendor relationships with the business.

OBRELA
SECURITY INDUSTRIES

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