

# HiSoftware Compliance Sheriff® Operational Security Module (OPSEC)

*Identify and manage online Operational Security vulnerabilities to ensure regulatory compliance*

## Benefits

- Identify problem areas
- Integrate Operational Security testing into your Quality Assurance and content delivery processes
- Measure and manage risk and compliance across the organization
- Custom Trend Analysis Reporting over time
- Allocate resources appropriately
- Track site progress

## **Risk Management - Operational Security**

The Internet age has revolutionized how organizations communicate, publish and find information. The Web provides organizations with a powerful tool to convey information quickly and efficiently on a broad range of topics relating to activities, objectives, policies and programs. While this technology has created new opportunities for global communication and commerce, it has also created new challenges in risk management.

Information placed on the Web, even with good intent, may provide for operational and security gaps that could put assets at risk. Troop movements, dignitary visits, power plant schematics, or an improper address or phone number, may create security issues that could be taken advantage of by a third party.

The volume of information available through organizational Web sites, intranets, extranets, and networks via multiple entry points, provided by multiple content contributors, in multiple forms and languages, has increased dramatically. The Internet is growing at a rate of 500,000 new World Wide Web entry points a month, providing vast resources of information to the public and to the adversary.

The potential for inadvertent or unauthorized disclosure of sensitive information continues to grow. Using search engines and information compilation algorithms, a single user can aggregate, analyze, and construct new levels of understanding from unclassified sources.

As such, risk assessment and risk management become critical factors in evaluating publicly accessible website information.

## **An Integrated System for Operational Security Testing**

Meet and manage all corporate website standards for accessibility, privacy, security, search engine optimization (SEO), brand consistency and marketing policies using HiSoftware Compliance Sheriff.

The Compliance Sheriff Operational Security Module provides an integrated solution for verification of accessible, usable, and searchable content that complies with Operational Security guidelines and Risk Assessment Practices. It provides a centralized system for mitigating online risk, and identifying and managing online operational security (OPSEC) vulnerabilities to ensure regulatory compliance.

## **With the Compliance Sheriff Operational Security Module organizations can:**

- Validate for compliance with OPSEC Standards and Guidelines.
- Manage content compliance efficiently and consistently throughout the content development and deployment lifecycles.
- Shorten Web publishing cycles by linking collaboration, publishing, and the online content audit processes.
- Customize Risk Management for checks, output, and reporting.
- Custom Trend Analysis Reporting over time.
- Work collaboratively with team members to ensure compliance with all standards.

With the Operational Security Module, Web Risk Assessment analysts and Web Managers are able to conduct automated and remote testing. The module automates the process of scanning, analyzing and reporting website security, privacy, usability, and compliance issues across departmental Web properties.



The Operational Security Module actively monitors websites and provides detailed reports allowing you to identify risk issues such as information collection, as well as provide the ability to track and monitor use of Keywords, key phrases, personal information and other "red flag" issues. Analysts can automate the process of testing and managing organization-wide Web compliance through the use and deployment of the Operational Security Module.

In combination with HiSoftware's AccVerify, you can also automate the verification of online compliance with Operational Security testing websites. These solutions assist organizations in testing for Operational Information, Personal Information and Technological Data.

## Reports

Reports available in the Operational Security Module include:

- *Website purpose statement*: Identifies that a website contains a clearly defined purpose statement that supports the mission of the DoD Component.
- *Page Titles*: A common method of search on both public and private sites is title searching. Important from an operational perspective, this check validates titles are present.
- *External Link Disclaimer*: Validates the website contains a Disclaimer for External Links notice when a user requests any site outside of the current Web information service.
- *Third party content or advertising*: This test validates no images are found that include third party content or advertising.
- *Operational Information - Lessons Learned Audit*: Identifies if the website contains any information indicating plans or lessons learned which would reveal military operations, exercises or vulnerabilities.
- *Operational Information - Military Information*: Determines if the website references any information that would reveal sensitive movements of military assets or the location of units, installations, or personnel where uncertainty regarding location is an element of the security of a military plan or program.
- *Personal Information*: Scans the site for personal information, about US citizens, DOD employees and military personnel; including Social Security number, Date of Birth, Address, Phone Number.
- *Technological Data - Schematic, Diagrams and Frequency*: Check for content containing any technical data, schematic diagrams, and the frequency of appearance.
- *Relevant Information*:
  - *Deployment, Exercise, Contingency or Training Schedules*: Identifies if the website contains relevant information that might reveal an organization's plans and intentions in the following categories, Administrative, Operational, Communications, and/or Logistics.
  - *Biographies, Family Support Activities and Phone Directories*: Searches for relevant information contained on the site that might reveal an organizations plans and intentions in the following categories Administrative, Operational, Communications and/or Logistics.

## System Requirements

### Client Browser

- Internet Explorer® version 6.0/7.0/8.0
- Mozilla Firefox® 2.0, 3.5 except for Transaction Path Recording and Local File Scanning
- Microsoft Windows® XP, 2000+, Windows Vista™, Windows 7

### Client HiSoftware Toolbar

- Internet Explorer version 6.0/7.0/8.0
- Microsoft .NET® Framework 2.0
- At least 1GB RAM and 2GB free disk space to run local scans

### Other File Format Support

- Microsoft Office® 2003 (required to scan Microsoft Word®, Excel®, Powerpoint®), Office 2007 and Adobe® PDF

### Server Requirements

- Microsoft Windows 2000/2003/2008 Server
- Internet Information sever 5.1 or greater
- Microsoft .NET Framework 2.0
- Windows Task Scheduler
- Microsoft SQL® Server 2000/2005/2008
- 4GB RAM or greater
- At least 5GB free disk space



### Corporate Headquarters

9 Trafalgar Square  
Nashua, NH 03063 USA

**Tel** 888.272.2484 (U.S. & Canada)  
+1.603.578.1870

**Fax** +1.603.578.1876

**Email** [info@hisoftware.com](mailto:info@hisoftware.com)

**[www.hisoftware.com](http://www.hisoftware.com)**

© Copyright 2010 HiSoftware Inc. All rights reserved.  
HiSoftware Compliance Sheriff and HiSoftware are registered trademarks of HiSoftware Inc. Any and all other product and company names mentioned herein are the trademarks or service marks of their respective owners.