

Benefits

- Comply with federal and international regulatory guidelines for best practices and risk management
- Increase your market share by making your Web site accessible to people with disabilities
- Avoid the risk of costly litigation, settlements and loss of business associated with not meeting compliance standards for accessibility and privacy
- Monitor sites for quality issues, including broken links, spelling, changed pages, and site up/down monitoring to promote the overall health of a Web site

Automating SharePoint Server Content Compliance

HiSoftware Compliance Sheriff for Microsoft SharePoint Server 2010/2007 complements SharePoint Server's powerful content publishing and collaborative features and functionality by providing users with a means to monitor content for potential compliance issues across their SharePoint sites – keeping information safe, within regulatory guidelines and appropriate. It provides a powerful platform for managing SharePoint content compliance to address Privacy, Accessibility, Social Media/Collaboration, Brand Consistency, Site Quality and Operational Security.

Once your SharePoint framework is made compliant, there are still many content components that change on a day to day basis:

- External and Internal websites edited
- Documents uploaded/edited
- Social collaboration through blogs/wikis
- Email communications

Compliance Sheriff makes managing this explosion of information easy with multiple options for monitoring content compliance:

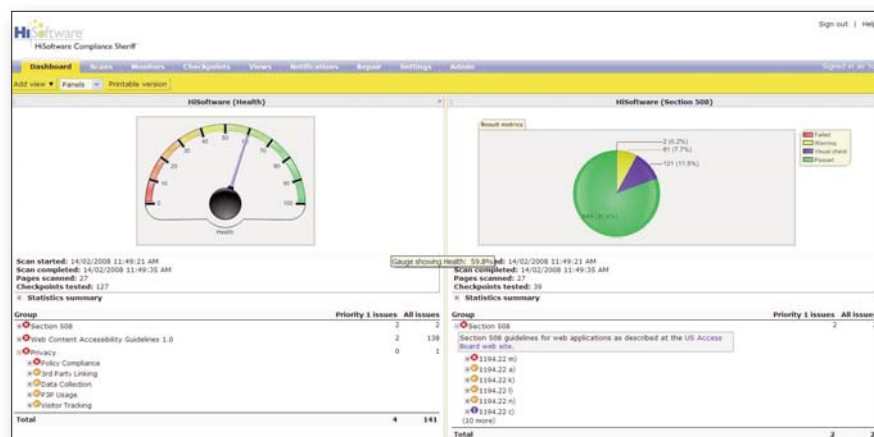
- Check content when it is created
- Scan it on-demand at the request of a user or administrator
- Monitor on scheduled intervals (every five minutes, daily, monthly, quarterly)

Compliance Sheriff for SharePoint

Offered as a HiSoftware-hosted or client-hosted subscription compliance management system, Compliance Sheriff validates Web content and applications against standards-based and organization-specific policies for privacy, accessibility, brand consistency, site quality, social media and collaboration, and operational security compliance. It enables an organization's policy managers to define policies and it provides a solution that empowers developers and content managers to validate compliance with these policies.

Compliance Sheriff provides testing and reporting options for standards-based Accessibility and Privacy policies based on the current standards outlined by Section 508, Section 208, and WCAG 1.0. and 2.0. Unlike other solutions, Compliance Sheriff allows users to easily define and test their organization's unique compliance policies without costly consulting and/or programming.

With Comprehensive Dashboard Reporting, content managers and executives can review current site status and site quality metrics over time. Web developers can drill down directly into pass/fail details for quick remediation. The result is a complete and concise report on the total accessibility, quality and policy compliance of a tested site, or pages of a site, that can be shared with the various groups responsible for Web Governance.



Above: Different views can be presented in a flexible and dynamic digital dashboard, providing end users, from executive management to developers, with a platform that easily communicates the status of your website(s).

Web-based Interface

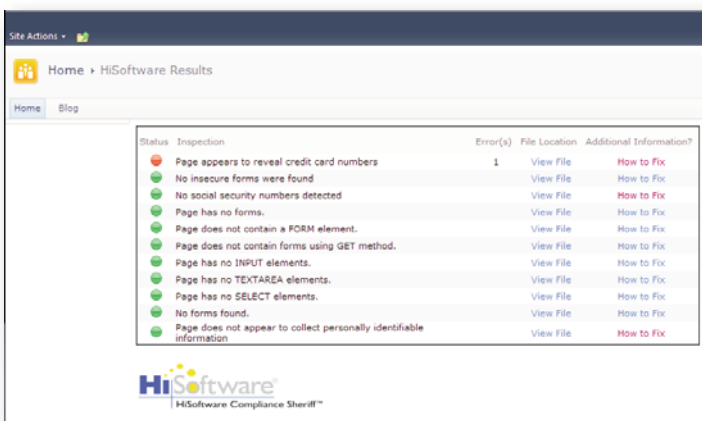
With Compliance Sheriff, a Web-based interface is used to schedule scans based on a number of preferences. Content can be scanned on-demand. Compliance Sheriff's administrative features allow administrators to create users and groups with unique rights and access to reporting and application features, helping manage usage. All users can test their content against applicable standards and benefit from comprehensive reporting.

Hosted Solution

Compliance Sheriff is available as an externally hosted solution through HiSoftware, or as a subscription that you install and host in-house on your own server. It can be scheduled to crawl and verify content every five minutes, daily, weekly or monthly. In addition, Compliance Sheriff can send email reports or links to the location of reports for all files verified or only those that fail compliance with specific rules. All reports are ready for distribution, including the "Web Ready" report that provides URL links to the files monitored and the corresponding reports, so anyone with a Web browser can view them. Compliance Sheriff can track files that reside on any server platform including: Linux, Windows, UNIX, Mac, Solaris, etc.

Integration into SharePoint

- Multiple workflows can be enabled for a site. This means that content can be blocked from being added to SharePoint if it does not meet a variety of criteria specified by the site's administrators.
- Detailed reports on a failure's location and the changes required to allow that content to be posted on the SharePoint site.
- Provides customizable help information on how to fix issues. Compliance Sheriff includes built-in help and customized help can be easily created.



Above left: View of a Compliance Report displayed within SharePoint.

Out-of-Box Compliance Standards Testing

HiSoftware Compliance Sheriff's Accessibility, Privacy, Brand Consistency, Site Quality and Operational Security options enable users to easily test for standards-based and custom factors with minimal configuration including:

Accessibility Compliance

- Section 508
- WCAG 1.0 and 2.0
- Common Look and Feel (CLF)
- XML Accessibility Guidelines (XAG)
- Any standard derived from WCAG or Section 508

Privacy Policy Compliance

Compliance Sheriff can report on a number of multi-national regulatory and compliance standards including:

- Children's Online Privacy Act (COPPA)
- Gramm-Leach Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- California SBI 386 and AB 1950
- Safe Harbor - EU
- Section 208 - US
- Privacy Act - US
- UK Data Protection Act
- Personal Information Protection and Electronic Documents Act - Canada (PIPEDA)
- EU Data Protection Directive 1995/46
- EU Privacy and Electronic Communications Directive 2002/58

Brand Consistency & Site Quality

This feature allows users to test for site quality and brand consistency issues including:

Technical Issues

- Site Up/Down status monitoring
- Link Validation with Links Analysis reports/view
- Slow loading pages

Content Errors

- Spell check using both primary and user/custom dictionaries
- Inappropriate language scanning
- Missing graphics

Marketing Issues

- Brand consistency
- Trademark usage
- Keywords for Search Engine Optimization (SEO)
- Hacked content via notification of modified pages

Social Media / Collaboration

Monitor inappropriate content, obscene language and posting of confidential information or personally identifiable information (PII) within a social or collaborative environment

like MySites, TeamSites, Blogs, Wikis and other social media tools. Leverages HR acceptable use policies to mitigate risk, protect the organization from potential harmful exposure, educate employees and improve behavior.

Operational Security - OPSEC

The Operational Security (OPSEC) module provides an integrated solution for compliance with OPSEC Guidelines and Risk Assessment Practices:

- Validate for compliance with OPSEC Standards and Guidelines
- Identify problem or exposed security areas
- Integrate Operational Security testing into your Quality Assurance and content delivery processes
- Measure and manage risk and compliance across the organization

Optional Accessibility Foundation Module (AFM)

AFM provides users with a set of tools to create an accessible platform/framework for a SharePoint portal or intranet site.

AFM is integrated into the Compliance Sheriff offering to provide a more complete and easy-to-deploy method of addressing SharePoint framework accessibility. The most significant advantage of AFM is the enterprise-friendly installation method that allows a SharePoint Server Administrator to easily apply a master configuration to multiple SharePoint Applications.

Workflow and Reporting

While a site administrator can check compliance at any time by manually initiating a scan, Compliance Sheriff's true power is in its ability to automate compliance, eliminating the need for human intervention. This is done through a combination of workflow and reporting:

Workflow

Compliance Sheriff can be configured to either block questionable content from being posted or allow the content to be posted while sending a notification to the site administrator. In either case, email notifications will be sent to site administrators and/or any other manager affected by the specific content – accessibility managers, privacy officers, marketing managers, etc. Email notifications can be scheduled to occur at any frequency, regardless of how often scans are run. Emails can include a whole report embedded directly within the email body so there's no need to be able to access the application. Examples of workflow include:

- When a user submits an improperly redacted document to the site, HiSoftware workflow identifies the improper redaction and notifies the site administrator.
- When a user sends an email or uploads a document exposing usernames or passwords, HiSoftware workflow notifies the site administrator and the IT security manager that a security breach has occurred.
- If personally identifiable information (PII) or protected health information (PHI) is mistakenly placed in a non-secure area of the site, HiSoftware Workflow blocks that placement, informs the user of the problem and notifies site management and the chief privacy officer.

- If heated debates are taking place on a team discussion forum, HiSoftware workflow will prevent offensive content (inappropriate language, slurs, etc.) from posting.
- If brand corruption occurs as a result of multiple logos or marketing messages in circulation, marketing managers will receive a notification, helping ensure websites maintain consistent branding and messaging.
- If a graphic does not meet Section 508 guidelines for accessibility, HiSoftware workflow will identify the Web content missing ALT text. The user will be prompted to add the needed text.

Reporting

HiSoftware Compliance Sheriff's Dashboard Reporting provides visual reports on compliance issues. The Dashboard gives IT managers the executive level summary reports they need to determine both the current compliance status and compliance trends over time. A detailed analysis for developers and quality assurance teams is a click away using the same highly customizable interface.

- Users can customize their own Dashboard to show just the results that interest them most by defining different "views" from either a single or multiple scans – without having to re-run the scan.
- Users can generate printable versions of the report summary for emailing, printing or archiving.
- Results can be viewed according to the user's preferred chart type including: Health Gauge, Page Compliance, Failures by Priority, Failures by Group, and Result Metrics.
- Charts can be plotted with a time axis, to show how your site's performance has changed over time.
- Statistics Summary Reports provide statistics on key elements such as Forms, Images, Scripts etc.
- Page Compliance and Issue Identification tables provide the ability to customize how the data is organized into various levels. A third, Links Analysis, provides a list of links identified across your website including the pages that link in and/or out of that page.
- Tables give a high level overview of site status with the ability to quickly drill down to exactly where a specific checkpoint failed on a specific page.

Custom Checkpoint Editor

In addition to universal compliance standards (WCAG, Section 508, HIPAA, etc.), many organizations have their own unique custom policy requirements. HiSoftware Compliance Sheriff includes a Custom Checkpoint Editor which allows users to easily define and validate against accessibility, privacy, brand consistency site quality and other custom checks that are required by your organization.

This extends the validation system provided in HiSoftware Compliance Sheriff to meet any specific need not covered by a publicly available standard or guideline. Test features, formats and customization can be pre-configured in HiSoftware Compliance Sheriff by an organization's policy managers so that developers, quality assurance professionals and other content creators within the organization can simply run these

programmatic tests and receive a result, without any requirement for software configuration. HiSoftware Compliance Sheriff's Custom Checkpoint Editor allows you to:

- View and edit the definition of each checkpoint from within the same application, so that out-of-the-box checkpoints can easily be tailored to meet each customer's needs.
- Configure almost infinitely complex checkpoint rules. For instance, a checkpoint can check for certain elements with certain attribute values but only on pages that contain particular text, or only on pages whose URLs match that particular criteria.
- Perform sophisticated pattern matching in checkpoint rules, to enable looking for very particular key pieces of data (e.g. credit card numbers, or input fields that appear to be asking for a user's real name, as opposed to a screen name or nickname).
- Groups and Subgroups allow for easier administration and management of checkpoints. For example, a checkpoint group assigned to a scan definition can be easily changed by adding or removing a Subgroup that contains several checkpoints, instead of individually adding/removing several checkpoints.

Scans - Web Application Testing

Defining a scan has never been simpler. A single scan definition can contain one or more domains, eliminating the need to run multiple scans for a single site. For example, by default, links to pages that reside on a different domain will be skipped; however, such domains can be added to the scan. You can even use the Include/Exclude filters to target specific pages in the additional domains, rather than crawling/scanning the entire domain.

Overview of Main Testing Features:

- Ability to bundle multiple domains into a single scan (as described above).
- Ability to schedule monitors that can be run automatically at regular intervals (minutes, hours, days, weeks, months). Monitors allow you to verify the quality of your website (site up/down, if pages or any of its resources have changed, identify slow pages) and send alerts based on the result of these tests and/or produce a report showing a history of the results.
- The Transaction Script Recorder allows Compliance Sheriff to simulate a user interacting with a transactional Web-based application (e.g. time and attendance system, resource management system, airline reservation system, online banking system) and incorporate accessibility, privacy and content quality testing into the interaction process.
- The scanning engine can automatically follow almost all types of links on a page, including those embedded inside JavaScript code. For links that can't be followed automatically (e.g. login screens, URL's constructed dynamically using JavaScript and submit forms), a transaction script can be used.
- Microsoft Office® and Adobe® documents (.DOC, DOCX, .XLS, XLSX, .PPT, PPTX, .PDF, .SWF and .MSG) can be validated for any compliance regulation including custom rules.
- Checking Cascading Style Sheets (CSS) and Accessible Rich Internet Applications (ARIA) markup for compliance errors. Easily specify what content is being used for decorative or purely presentation purposes in content.
- For areas where manual verification is required, the Compliance Sheriff Results Revision Wizard will easily enable an audit trail to be created that allows content reviewers to pass or fail content and provide justification for doing so that can be included in reports.

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

- Windows SharePoint Services 3, Microsoft Office SharePoint® Server 2007, Microsoft SharePoint Server 2010
- Microsoft Windows 2003/2008 Server
- Internet Information Server 5.1 or greater
- Microsoft .NET Framework 2.0
- Windows Task Scheduler
- Microsoft SQL® Server 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

www.hisoftware.com