# Comprehensive STIG Management Platform

Strategic STIG Automation and Workflow Engine that transforms manual STIG management into an intelligent, automated compliance system, reducing STIG evaluation time by 90% while improving accuracy and consistency through AI-powered automation and comprehensive workflow management.

## 🎯 Overview

The STIG Management Platform provides: - **STIG Library Integration** - Direct integration with DISA STIG repositories for automated download and updates - **Native STIG Viewer** - Built-in STIG viewing capabilities eliminating dependency on external applications - **Workflow Automation** - Customizable workflows for STIG assignment, evaluation, review, and approval - **AI-Powered Assistance** - Intelligent guidance for implementation, remediation, and automation - **Automated Hardening** - Comprehensive system hardening with backup and rollback capabilities - **Progress Tracking** - Real-time visibility into STIG evaluation progress across all systems - **Compliance Reporting** - Advanced analytics and compliance reporting with trend analysis

## 🏗️ Database Schema

### Core Tables

-- STIG Library: Master repository of STIG rules and guidance  
stig\_library (id, stig\_id, title, description, version, release\_date, category,  
 severity, status, implementation\_guidance, verification\_text,  
 risk\_assessment, platforms, ref\_links, check\_content, fix\_text,  
 cci\_references, nist\_references, stig\_benchmark, rule\_id, vuln\_id,  
 group\_id, weight, ia\_controls, automation\_supported,  
 requires\_manual\_review, estimated\_fix\_time, business\_impact,  
 technical\_complexity, prerequisites, compliance\_frameworks,  
 tags, metadata, created\_at, updated\_at)  
  
-- STIG Checklists: Asset-specific STIG evaluation checklists  
stig\_checklists (id, asset\_id, benchmark\_id, title, version, release\_info,  
 status, target\_type, findings, total\_rules, completed\_rules,  
 open\_findings, not\_applicable, compliant\_findings,  
 non\_compliant\_findings, assigned\_to, reviewed\_by, reviewed\_at,  
 approved\_by, approved\_at, due\_date, priority, estimated\_effort,  
 actual\_effort, compliance\_score, risk\_score, workflow\_state,  
 escalation\_level, business\_justification, technical\_justification,  
 compensating\_controls, residual\_risk, mitigation, metadata,  
 created\_by, created\_at, updated\_at)  
  
-- STIG Assessments: Individual STIG rule assessments  
stig\_assessments (id, asset\_id, stig\_id, checklist\_id, status, assessment\_date,  
 assessment\_details, finding\_details, implementation\_status,  
 compliance\_status, compliance\_date, assigned\_to, assessed\_by,  
 reviewed\_by, approved\_by, mitigation\_plan, remediation\_date,  
 verification\_method, finding\_type, severity, impact, likelihood,  
 risk\_rating, business\_impact, technical\_impact,  
 compensating\_controls, residual\_risk, exception\_request,  
 automated\_check, manual\_override, workflow\_state,  
 escalation\_level, sla\_deadline, priority, effort, cost,  
 metadata, created\_at, updated\_at)  
  
-- STIG Scan Results: Automated scan results  
stig\_scan\_results (id, asset\_id, scan\_date, scan\_tool, scan\_version,  
 scan\_profile, compliance\_score, total\_checks, passed\_checks,  
 failed\_checks, not\_applicable\_checks, critical\_findings,  
 high\_findings, medium\_findings, low\_findings, findings,  
 raw\_results, scan\_duration, scan\_status, error\_message,  
 baseline\_id, delta\_from\_baseline, trend\_data, scheduled\_scan,  
 scan\_triggered\_by, notifications\_sent, report\_generated,  
 report\_path, metadata, created\_at, updated\_at)  
  
-- STIG Hardening Sessions: Automated hardening sessions  
stig\_hardening\_sessions (id, session\_id, target\_host, platform, platform\_version,  
 hardening\_profile, start\_time, end\_time, status,  
 compliance\_score, pre\_hardening\_score, post\_hardening\_score,  
 total\_rules, applied\_rules, failed\_rules, skipped\_rules,  
 backup\_created, backup\_path, rollback\_available, dry\_run,  
 force\_mode, continue\_on\_error, initiated\_by, approved\_by,  
 approved\_at, scheduled\_for, priority, business\_justification,  
 change\_request\_id, maintenance\_window, rollback\_plan,  
 testing\_plan, risk\_assessment, impact\_analysis,  
 success\_criteria, notes, error\_log, execution\_log,  
 performance\_metrics, resource\_usage, notifications,  
 metadata, created\_at, updated\_at)  
  
-- STIG Hardening Results: Individual rule hardening results  
stig\_hardening\_results (id, session\_id, rule\_id, stig\_id, status, before\_state,  
 after\_state, execution\_time, error\_message, warning\_message,  
 backup\_location, requires\_reboot, requires\_logoff,  
 service\_restart\_required, services\_affected, files\_modified,  
 registry\_keys\_modified, permissions\_changed,  
 configuration\_changes, validation\_result, validation\_details,  
 rollback\_available, rollback\_tested, impact\_assessment,  
 risk\_level, business\_impact, user\_impact, performance\_impact,  
 security\_improvement, compliance\_improvement,  
 automation\_confidence, manual\_verification\_required,  
 post\_implementation\_testing, monitoring\_recommendations,  
 maintenance\_requirements, documentation\_updates,  
 training\_requirements, communication\_needs, metadata,  
 created\_at, updated\_at)  
  
-- STIG Hardening Backups: Backup information for rollback  
stig\_hardening\_backups (id, session\_id, rule\_id, backup\_path, backup\_type,  
 target\_host, backup\_size, compression\_used, encryption\_used,  
 checksum\_md5, checksum\_sha256, backup\_method, backup\_tool,  
 backup\_version, original\_path, original\_permissions,  
 original\_owner, original\_size, original\_modified,  
 backup\_description, restore\_instructions, restore\_priority,  
 restore\_order, dependencies, expires\_at, is\_restored,  
 restored\_at, restored\_by, restore\_result, restore\_notes,  
 verification\_status, verified\_at, verified\_by,  
 retention\_policy, storage\_location, storage\_type,  
 access\_permissions, audit\_trail, metadata,  
 created\_at, updated\_at)  
  
-- STIG Fix Status: Track individual STIG rule fix status  
stig\_fix\_status (id, stig\_id, rule\_id, asset\_id, user\_id, assessment\_id,  
 checklist\_id, is\_completed, completed\_at, fix\_method,  
 fix\_duration, fix\_complexity, fix\_cost, business\_impact,  
 downtime, rollback\_tested, rollback\_time, verification\_method,  
 verification\_result, verified\_by, verified\_at, approved\_by,  
 approved\_at, implementation\_date, scheduled\_date, priority,  
 status, workflow\_state, assigned\_team, escalation\_level,  
 sla\_deadline, change\_request\_id, testing\_results,  
 quality\_assurance, documentation\_updated, training\_provided,  
 communication\_sent, monitoring\_enabled, alerts\_configured,  
 backup\_verified, rollback\_plan, contingency\_plan,  
 lessons\_learned, best\_practices, recommendations, notes,  
 attachments, tags, metadata, created\_at, updated\_at)  
  
-- STIG AI Assistance: AI-powered STIG guidance and automation  
stig\_ai\_assistance (id, stig\_id, asset\_id, assessment\_id, user\_id, request\_type,  
 question, context, system\_context, environment\_context,  
 compliance\_context, implementation\_guidance, remediation\_plan,  
 automation\_script, testing\_procedure, rollback\_procedure,  
 risk\_assessment, business\_impact, technical\_impact,  
 cost\_estimate, time\_estimate, complexity\_score,  
 confidence\_score, ai\_provider, ai\_model, ai\_response,  
 ai\_metadata, prompt\_used, tokens\_used, processing\_time,  
 quality\_rating, user\_feedback, implementation\_status,  
 implementation\_result, validation\_result, effectiveness\_score,  
 accuracy\_score, usefulness\_score, follow\_up\_required,  
 follow\_up\_notes, related\_requests, tags, is\_public,  
 is\_approved, approved\_by, approved\_at, version,  
 parent\_request\_id, metadata, created\_at, updated\_at)

### Relationships

Users ←→ StigLibrary (created\_by)  
Users ←→ StigChecklists (created\_by, assigned\_to, reviewed\_by, approved\_by)  
Users ←→ StigAssessments (assigned\_to, assessed\_by, reviewed\_by, approved\_by)  
Users ←→ StigScanResults (scan\_triggered\_by)  
Users ←→ StigHardeningSessions (initiated\_by, approved\_by)  
Users ←→ StigFixStatus (user\_id, verified\_by, approved\_by)  
Users ←→ StigAiAssistance (user\_id, approved\_by)  
  
Assets ←→ StigChecklists (asset\_id)  
Assets ←→ StigAssessments (asset\_id)  
Assets ←→ StigScanResults (asset\_id)  
Assets ←→ StigFixStatus (asset\_id)  
Assets ←→ StigAiAssistance (asset\_id)  
  
StigLibrary ←→ StigAssessments (stig\_id)  
StigLibrary ←→ StigHardeningResults (stig\_id)  
StigLibrary ←→ StigFixStatus (stig\_id)  
StigLibrary ←→ StigAiAssistance (stig\_id)  
  
StigChecklists ←→ StigAssessments (checklist\_id)  
StigChecklists ←→ StigFixStatus (checklist\_id)  
  
StigAssessments ←→ StigFixStatus (assessment\_id)  
StigAssessments ←→ StigAiAssistance (assessment\_id)  
  
StigHardeningSessions ←→ StigHardeningResults (session\_id)  
StigHardeningSessions ←→ StigHardeningBackups (session\_id)

## 📊 STIG Categories and Severity Levels

### STIG Categories

const STIG\_CATEGORIES = [  
 'operating\_system', // OS-specific STIGs (Windows, Linux, etc.)  
 'database', // Database STIGs (Oracle, SQL Server, etc.)  
 'web\_server', // Web server STIGs (Apache, IIS, etc.)  
 'network\_device', // Network device STIGs (Cisco, Juniper, etc.)  
 'virtualization', // Virtualization STIGs (VMware, Hyper-V, etc.)  
 'directory\_service', // Directory service STIGs (Active Directory, etc.)  
 'application', // Application-specific STIGs  
 'mobile\_device', // Mobile device STIGs  
 'cloud\_service', // Cloud service STIGs  
 'other' // Other/miscellaneous STIGs  
];

### Severity Levels

const STIG\_SEVERITY\_LEVELS = [  
 'low', // CAT III - Low risk  
 'medium', // CAT II - Medium risk  
 'high', // CAT I - High risk  
 'critical' // Critical - Immediate attention required  
];

### Status Types

const STIG\_STATUS\_TYPES = [  
 'active', // Currently active and applicable  
 'deprecated', // Deprecated but may still be referenced  
 'draft', // Draft version not yet finalized  
 'superseded' // Replaced by newer version  
];

## 🔄 STIG Workflow States

### Checklist Workflow

const CHECKLIST\_WORKFLOW = {  
 'not\_started': {  
 description: 'Checklist created but not yet started',  
 nextStates: ['in\_progress', 'cancelled'],  
 permissions: ['stig:write']  
 },  
 'in\_progress': {  
 description: 'Checklist evaluation in progress',  
 nextStates: ['completed', 'on\_hold', 'cancelled'],  
 permissions: ['stig:write']  
 },  
 'completed': {  
 description: 'All checklist items completed',  
 nextStates: ['reviewed', 'in\_progress'],  
 permissions: ['stig:write']  
 },  
 'reviewed': {  
 description: 'Checklist reviewed by supervisor',  
 nextStates: ['approved', 'rejected', 'in\_progress'],  
 permissions: ['stig:review']  
 },  
 'approved': {  
 description: 'Checklist approved and finalized',  
 nextStates: ['archived'],  
 permissions: ['stig:approve']  
 },  
 'rejected': {  
 description: 'Checklist rejected, requires rework',  
 nextStates: ['in\_progress', 'cancelled'],  
 permissions: ['stig:approve']  
 }  
};

### Assessment Workflow

const ASSESSMENT\_WORKFLOW = {  
 'pending': {  
 description: 'Assessment assigned but not started',  
 nextStates: ['in\_progress', 'cancelled'],  
 permissions: ['stig:write']  
 },  
 'in\_progress': {  
 description: 'Assessment being conducted',  
 nextStates: ['completed', 'on\_hold', 'cancelled'],  
 permissions: ['stig:write']  
 },  
 'completed': {  
 description: 'Assessment completed',  
 nextStates: ['reviewed', 'in\_progress'],  
 permissions: ['stig:write']  
 },  
 'reviewed': {  
 description: 'Assessment reviewed',  
 nextStates: ['approved', 'rejected', 'in\_progress'],  
 permissions: ['stig:review']  
 },  
 'approved': {  
 description: 'Assessment approved',  
 nextStates: ['implemented', 'exception\_requested'],  
 permissions: ['stig:approve']  
 },  
 'rejected': {  
 description: 'Assessment rejected',  
 nextStates: ['in\_progress', 'cancelled'],  
 permissions: ['stig:approve']  
 }  
};

## 🤖 AI-Powered STIG Assistance

### AI Request Types

const AI\_REQUEST\_TYPES = [  
 'guidance', // Implementation guidance and best practices  
 'automation', // Automation script generation  
 'analysis', // Risk and impact analysis  
 'remediation', // Remediation planning and procedures  
 'testing', // Testing and validation procedures  
 'documentation', // Documentation generation  
 'training' // Training material generation  
];

### AI Assistance Features

const AI\_ASSISTANCE\_FEATURES = {  
 implementation\_guidance: {  
 description: 'Generate step-by-step implementation guidance',  
 inputs: ['stig\_rule', 'system\_context', 'environment\_details'],  
 outputs: ['detailed\_steps', 'prerequisites', 'validation\_methods']  
 },  
 automation\_scripts: {  
 description: 'Generate automation scripts for STIG implementation',  
 inputs: ['stig\_rule', 'platform', 'scripting\_language'],  
 outputs: ['script\_code', 'execution\_instructions', 'rollback\_procedures']  
 },  
 risk\_assessment: {  
 description: 'Analyze risk and business impact',  
 inputs: ['stig\_rule', 'business\_context', 'system\_criticality'],  
 outputs: ['risk\_analysis', 'business\_impact', 'mitigation\_strategies']  
 },  
 remediation\_planning: {  
 description: 'Create comprehensive remediation plans',  
 inputs: ['findings', 'resources', 'timeline'],  
 outputs: ['remediation\_plan', 'resource\_requirements', 'timeline\_estimates']  
 }  
};

## 🔧 Automated Hardening Engine

### Hardening Session Types

const HARDENING\_SESSION\_TYPES = {  
 'assessment\_only': {  
 description: 'Assessment without making changes',  
 risk\_level: 'low',  
 backup\_required: false  
 },  
 'guided\_hardening': {  
 description: 'Interactive hardening with user approval',  
 risk\_level: 'medium',  
 backup\_required: true  
 },  
 'automated\_hardening': {  
 description: 'Fully automated hardening',  
 risk\_level: 'high',  
 backup\_required: true  
 },  
 'emergency\_hardening': {  
 description: 'Emergency hardening for critical vulnerabilities',  
 risk\_level: 'critical',  
 backup\_required: true  
 }  
};

### Backup Types

const BACKUP\_TYPES = [  
 'file', // File system backups  
 'registry', // Windows registry backups  
 'configuration', // Configuration file backups  
 'service', // Service configuration backups  
 'permission', // Permission and ACL backups  
 'full\_system' // Full system state backup  
];

## 📈 Analytics and Reporting

### Key Performance Indicators (KPIs)

const STIG\_KPIS = {  
 compliance\_metrics: {  
 overall\_compliance\_rate: 'Percentage of compliant STIG rules',  
 compliance\_by\_severity: 'Compliance rates by severity level',  
 compliance\_by\_category: 'Compliance rates by STIG category',  
 compliance\_trends: 'Compliance trends over time'  
 },  
 operational\_metrics: {  
 assessment\_completion\_rate: 'Percentage of completed assessments',  
 average\_assessment\_time: 'Average time to complete assessments',  
 remediation\_time: 'Average time to remediate findings',  
 automation\_rate: 'Percentage of automated implementations'  
 },  
 quality\_metrics: {  
 finding\_accuracy: 'Accuracy of automated findings',  
 false\_positive\_rate: 'Rate of false positive findings',  
 manual\_override\_rate: 'Rate of manual overrides',  
 review\_rejection\_rate: 'Rate of rejected reviews'  
 },  
 resource\_metrics: {  
 effort\_estimation\_accuracy: 'Accuracy of effort estimates',  
 cost\_per\_assessment: 'Average cost per assessment',  
 resource\_utilization: 'Resource utilization rates',  
 training\_effectiveness: 'Training program effectiveness'  
 }  
};

### Compliance Reporting

const COMPLIANCE\_REPORTS = {  
 executive\_dashboard: {  
 description: 'High-level compliance overview for executives',  
 frequency: 'monthly',  
 recipients: ['executives', 'compliance\_officers'],  
 metrics: ['overall\_compliance', 'risk\_trends', 'resource\_allocation']  
 },  
 technical\_assessment: {  
 description: 'Detailed technical assessment report',  
 frequency: 'weekly',  
 recipients: ['security\_team', 'system\_administrators'],  
 metrics: ['detailed\_findings', 'remediation\_status', 'technical\_recommendations']  
 },  
 audit\_report: {  
 description: 'Comprehensive audit report for external auditors',  
 frequency: 'quarterly',  
 recipients: ['auditors', 'compliance\_team'],  
 metrics: ['compliance\_evidence', 'control\_effectiveness', 'audit\_trail']  
 },  
 trend\_analysis: {  
 description: 'Trend analysis and predictive insights',  
 frequency: 'monthly',  
 recipients: ['management', 'security\_team'],  
 metrics: ['compliance\_trends', 'risk\_predictions', 'improvement\_recommendations']  
 }  
};

## 🚀 API Endpoints

### STIG Library Management (8 endpoints)

// STIG Library CRUD operations  
POST /api/v1/stig/library // Create STIG library entry  
GET /api/v1/stig/library // Get all STIG library entries with filtering  
GET /api/v1/stig/library/:stigId // Get STIG library entry by ID  
PUT /api/v1/stig/library/:stigId // Update STIG library entry  
DELETE /api/v1/stig/library/:stigId // Delete STIG library entry  
  
// STIG Import and Download  
POST /api/v1/stig/import/xml // Import STIG from XML file  
POST /api/v1/stig/download/disa // Download STIG from DISA repository  
  
// Analytics  
GET /api/v1/stig/analytics // Get STIG analytics and statistics

### STIG Checklist Management (6 endpoints)

// Checklist CRUD operations  
POST /api/v1/stig/checklists // Create STIG checklist  
GET /api/v1/stig/checklists // Get all STIG checklists with filtering  
GET /api/v1/stig/checklists/:checklistId // Get STIG checklist by ID  
PUT /api/v1/stig/checklists/:checklistId // Update STIG checklist  
DELETE /api/v1/stig/checklists/:checklistId // Delete STIG checklist  
  
// Checklist Operations  
POST /api/v1/stig/checklists/:checklistId/assign // Assign checklist to user

## 🛠️ Usage Examples

### Creating a STIG Library Entry

const stigData = {  
 stigId: 'RHEL-07-010010',  
 title: 'The Red Hat Enterprise Linux operating system must be configured so that the file permissions, ownership, and group membership of system files and commands match the vendor values.',  
 description: 'Discretionary access control is weakened if a user or group has access permissions to system files and directories greater than the default.',  
 version: '1.0',  
 releaseDate: '2023-01-15',  
 category: 'operating\_system',  
 severity: 'high',  
 status: 'active',  
 platforms: ['linux', 'rhel'],  
 checkContent: 'Verify the file permissions, ownership, and group membership of system files and directories match the vendor values...',  
 fixText: 'Run the following command to reset the permissions and ownership of system files...',  
 cciReferences: ['CCI-001499'],  
 nistReferences: ['CM-5 (6)', 'SI-7'],  
 stigBenchmark: 'RHEL\_7\_STIG',  
 ruleId: 'SV-86473r2\_rule',  
 vulnId: 'V-61849',  
 groupId: 'V-61849',  
 weight: 5.0,  
 automationSupported: true,  
 requiresManualReview: false,  
 estimatedFixTime: 30,  
 businessImpact: 'medium',  
 technicalComplexity: 'low',  
 prerequisites: ['root\_access', 'system\_backup'],  
 complianceFrameworks: ['NIST', 'DISA', 'FISMA'],  
 tags: ['file\_permissions', 'system\_integrity', 'access\_control']  
};  
  
const stig = await stigService.createStigLibraryEntry(stigData, userId);

### Creating a STIG Checklist

const checklistData = {  
 assetId: 123,  
 benchmarkId: 'RHEL\_7\_STIG',  
 title: 'RHEL 7 STIG Checklist - Production Server',  
 version: '1.0',  
 releaseInfo: 'Release 1.0 - January 2023',  
 targetType: 'linux\_server',  
 assignedTo: 456,  
 dueDate: '2024-02-15T23:59:59Z',  
 priority: 'high',  
 estimatedEffort: 40,  
 scanFrequency: 'weekly',  
 automatedScanEnabled: true,  
 businessJustification: 'Critical production server requiring STIG compliance for security certification',  
 technicalJustification: 'Server hosts sensitive financial data and requires enhanced security controls',  
 metadata: {  
 environment: 'production',  
 businessUnit: 'finance',  
 dataClassification: 'confidential',  
 complianceDeadline: '2024-03-01'  
 }  
};  
  
const checklist = await stigService.createStigChecklist(checklistData, userId);

### Advanced Filtering and Search

// Get STIG library entries with complex filtering  
const stigs = await stigService.getAllStigLibraryEntries({  
 category: 'operating\_system',  
 severity: 'high',  
 status: 'active',  
 platform: 'linux',  
 search: 'file permissions'  
}, {  
 page: 1,  
 limit: 20,  
 sortBy: 'severity',  
 sortOrder: 'desc'  
});  
  
console.log(`Found ${stigs.pagination.totalCount} matching STIGs`);  
stigs.data.forEach(stig => {  
 console.log(`- ${stig.stigId}: ${stig.title} (${stig.severity})`);  
});

### Getting STIG Analytics

const analytics = await stigService.getStigAnalytics();  
  
console.log('STIG Library Statistics:');  
console.log(`- Total STIGs: ${analytics.library.total}`);  
console.log(`- Active STIGs: ${analytics.library.active}`);  
console.log(`- Critical STIGs: ${analytics.library.critical}`);  
console.log(`- High STIGs: ${analytics.library.high}`);  
  
console.log('\nChecklist Statistics:');  
console.log(`- Total Checklists: ${analytics.checklists.total}`);  
console.log(`- In Progress: ${analytics.checklists.inProgress}`);  
console.log(`- Completed: ${analytics.checklists.completed}`);  
console.log(`- Approved: ${analytics.checklists.approved}`);  
  
console.log('\nAssessment Statistics:');  
console.log(`- Total Assessments: ${analytics.assessments.total}`);  
console.log(`- Compliant: ${analytics.assessments.compliant}`);  
console.log(`- Non-Compliant: ${analytics.assessments.nonCompliant}`);  
console.log(`- Not Applicable: ${analytics.assessments.notApplicable}`);

## 🔒 Security and Compliance Features

### Access Control

const stigPermissions = {  
 'stig:read': 'View STIG library, checklists, and assessments',  
 'stig:write': 'Create and update STIG assessments and checklists',  
 'stig:review': 'Review and validate STIG assessments',  
 'stig:approve': 'Approve STIG assessments and grant exceptions',  
 'stig:admin': 'Manage STIG library, import STIGs, and configure system',  
 'stig:automate': 'Execute automated hardening and remediation',  
 'stig:audit': 'Access audit logs and compliance reports'  
};

### Data Protection

const dataProtection = {  
 encryption: {  
 atRest: 'AES-256 encryption for sensitive STIG data',  
 inTransit: 'TLS 1.3 for all API communications',  
 backups: 'Encrypted backups with key rotation'  
 },  
 access\_controls: {  
 authentication: 'Multi-factor authentication required',  
 authorization: 'Role-based access control (RBAC)',  
 session\_management: 'Secure session handling with timeout'  
 },  
 compliance: {  
 frameworks: ['NIST', 'DISA', 'FISMA', 'FedRAMP'],  
 certifications: ['SOC 2', 'ISO 27001'],  
 auditing: 'Comprehensive audit logging and monitoring'  
 }  
};

This comprehensive STIG Management Platform provides enterprise-grade STIG automation and workflow management capabilities with advanced AI assistance, automated hardening, and robust compliance reporting for modern cybersecurity operations.