"FISMA requires each federal agency to develop, document, and implement an agency-wide program to provide security for the information and systems..."

"Gartner research says that 80% of unplanned downtime is due to people and process issues."

"...ChangeGear simplifies change control and gives you the tools you need to track, manage, and control your critical infrastructure."

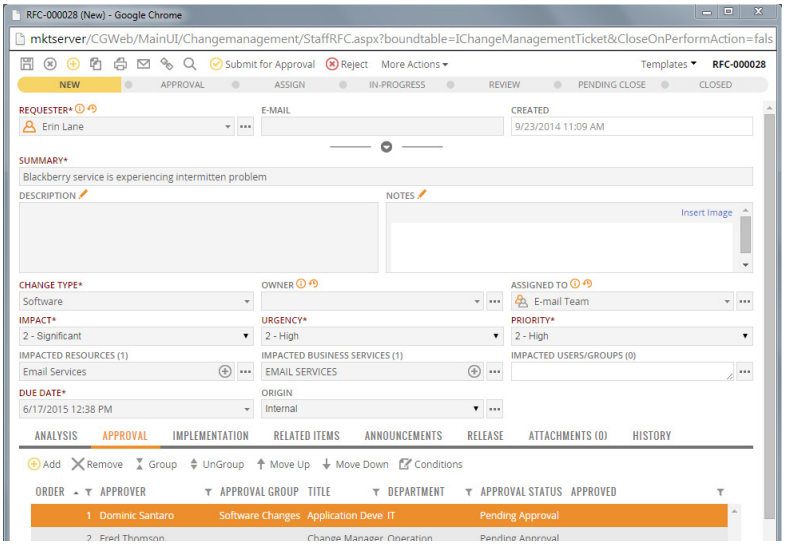
Change and Configuration Management for Government

Simplify Compliance with Federal Regulations and Standards

About FISMA & NIST

The Federal Information Security Management Act (FISMA) is a federal law enacted in 2002 to recognize the importance of information security to the economic and national security interests of the United States. FISMA requires each federal agency to develop, document, and implement an agency-wide program to provide security for the information and systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

To strengthen information system security, FISMA assigns specific responsibilities to a federal agency called the National Institute of Standards and Technology (NIST). In particular, FISMA requires NIST to help implement policies and procedures that cost-effectively reduce information technology security risks to an acceptable level. NIST works with federal agencies to improve their understanding of FISMA compliance by publishing standards and guidelines which provide the foundation for strong information security programs.



NIST Provides Configuration Guidelines for Managing Risk

Both FISMA and the associated NIST standards are driving all IT departments of federal agencies to adopt a security risk management approach and to implement automation tools that ensure systems are meeting baseline requirements. This approach requires accurate reporting of inventory and security controls, as well as the ability to effectively control configuration change.

While FISMA outlines a comprehensive structure for establishing an information security program, it is up to the organization to implement its directives in a manner that provides adequate security for protecting information and information systems. As threats continue to evolve in an environment where organizations have limited resources with which to protect themselves, security has become a risk-based activity. Operational and economic costs of ensuring security must be balanced against the needs of the organization.

Recently, NIST has issued Special Publication 800-128, which is a new draft set of minimum security configuration guidelines for government infrastructures that helps agencies plan and apply effective security configurations. The publication describes guidelines "for managing the configuration of the information system architecture and associated components for secure processing, storing, and transmitting of information." In this document, NIST provides fundamental concepts of Security Configuration Management (SCM) and offers insight into developing policies and procedures.

Contact Us

Phone: 800.390.4169
Sales: 813.840.4027
Email: Sales@SunViewSoftware.com
www.SunViewSoftware.com

SunView Software Inc.

Automate NIST Guidelines to Simplify Compliance

It is possible to meet the key provisions of the NIST guidelines using manual tracking and management, but it can be time-consuming, labor-intensive, and inefficient. This is the reason why so many agencies choose an effective change and configuration management software solution to help achieve compliance.

Change and Configuration Management software can simplify the management of your critical systems and configuration items by providing security enforcement, process documentation, workflow automation, and reporting capabilities for audits. Based on NIST, below are key concepts that should be in place for managing risk and ensuring the security of your IT infrastructure:

NIST Guideline	Description
Change Control Board	The Change Control Board establishment is part of the Planning phase of (SCM) and supports the implementation of NIST SP 800-53 control CM-3 Configuration Change Control.
Information System Component Inventory	Creating an inventory of IS components for an information system is part of the Planning phase and supports the implementation of the NIST SP 800-53 control CM-8 Information System Component Inventory. Change and Configuration Management Software can automate the initial discovery of IS assets, allow for the assignment of a system or individual asset owner, and provide a consolidated and reportable representation of all components.
Configuration Items	Identification of the configuration items that compose an information system is part of the Planning phase of SCM and supports the implementation of NIST SP 800-53 control CM-3 Configuration Change Control. Change and Configuration Management Software allows you to identify, label, and track the life cycle of each configuration item. This includes the management of all activities within SCM, such as configurations, relationships, change control, and change monitoring.
Secure Configurations of Information Systems	Implementing secure configurations is part of the Configure to Secure State phase of SCM and supports the implementation of NIST SP 800-53 controls CM-6 Configuration Settings and CM-7 Least Functionality. Change and Configuration Management Software helps manage secure configurations of the IS infrastructure with automated configuration scanning and visual mapping of configuration items, their dependencies, and relationships.
Baseline Configuration	Developing and documenting the baseline configuration for an information system is part of the Configuring to a Secure State phase of SCM and supports the implementation of NIST SP 800-53 control CM-2 Baseline Configuration. Change and Configuration Management Software allows you to maintain all aspects of approved configuration details such as processes running, open ports, current software installed, and configuration of the individual components.
Configuration Change Control	Configuration change control falls under the Maintaining Secure State phase of SCM and supports the implementation of NIST SP 800-53 control CM-3 Configuration Change Control and CM-5 Access Restrictions for Change. Change and Configuration Management Software helps you implement a secure process of change control for tracking modifications, additions, or the removal of configuration items within your infrastructure.
Security Impact Analysis	Security impact analysis is performed as a part of the Maintaining Secure State phase of SCM and supports the implementation of NIST SP 800-53 control CM-4 Security Impact Analysis. Change and Configuration Management Software allows you to manage the risk and vulnerability of configuration items. With current configuration information at your fingertips, an impact analysis can be done prior to change to be sure that the systems are not negatively affected.
Configuration Monitoring	Configuration compliance activities are an important part of the Monitoring phase of SCM and support the implementation of all NIST SP 800-53 controls in the CM Family. Change and Configuration Management Software can automate the scanning of software and hardware configuration changes then make comparisons to your baseline. Once a configuration change is identified, staff can be notified of the configuration change.

SunView Software Inc.

Change Management

ChangeGear's Change Management ensures that every change introduced into the IT infrastructure follows a regulated process. The following key features can be found in the Change Management solution:

ChangeGear Feature	Description
Change Control	ChangeGear enables IT organizations to track, manage, and control all aspects of the change lifecycle, from approving change requests and notifying stakeholders to analyzing the risk and impact of change to the IT infrastructure.
Dynamic Request Automation	ChangeGear allows for intelligent handling of requests that leverage the power of customized forms, advanced workflows, notifications, and approvals. Form authoring tools give you complete control of the layout, labels, what fields are displayed on the ticket, actions, and workflows.
Automated Approvals & Notifications	ChangeGear's customizable approval and notification system automates communication by enforcing your pre-designed approval structure and ensuring that the right team members are notified at each stage in the change lifecycle: before, during, and after change.
Process and Workflow Automation	ChangeGear allows agencies to define their own change management processes and automate the way they want to work using the power of workflow automation. This ensures compliance, enforces best practices, streamlines performance, and guarantees repeatable outcomes.
Change Monitoring	ChangeGear provides built-in and definable Business Policy Automation tools that can monitor hardware and software changes on datacenter assets. Once an unauthorized system change is found, ChangeGear can send an alert to the owner of network access or initiate the appropriate action.
Change and Audit Reporting	ChangeGear tracks all aspects of historical and current change activity in the organization: change status, cost, impacted resources, priority/category of change, and change by user or department. ChangeGear gives you access to real-time and comprehensive compliance reports for auditors.

Configuration Management

ChangeGear's Configuration Management Database (CMDB) allows you to discover, manage, and monitor all of your datacenter assets and configuration items. The following key features can be found in the CMDB solution:

ChangeGear Feature	Description
Auto-Discovery of Datacenter Assets and Configuration Items	ChangeGear provides a comprehensive solution for collecting and managing IT assets and configuration items, both physical and virtual. Using agentless and dynamic probing methods, ChangeGear gives you a 360-degree view into your IT infrastructure by automatically discovering applications, servers, and many other network devices.
Asset and Configuration Management	ChangeGear gives IT organizations greater control of datacenter assets throughout their operational lifecycles – providing auto-discovery, configuration information, storage of documentation, and many other miscellaneous details for each configuration item.
CMDB Extensibility	In addition to managing IT assets such as routers and servers, ChangeGear provides you the ability to easily add new asset types to track non-datacenter resources such as generators or other various equipment. The form authoring tools give you complete control of the layout, labels, and what fields are displayed on the custom form.
Risk Management and Impact Analysis	ChangeGear delivers unparalleled visibility into the IT infrastructure by providing configuration information and visual mappings of datacenter assets and resources, as well as their dependencies and relationships. This is critical for in-depth impact analysis, risk assessments, troubleshooting, and root-cause analysis.
Reporting	ChangeGear captures a complete audit-trial of changes and services for each datacenter asset – then provides a number of pre-defined reports out of the box to meet compliance requirements. Customized reports can also be created with ChangeGear's easy-to-use ad-hoc reporting tools.
Federated Database	ChangeGear is built on a federated data model; it consolidates and centralizes information from various data sources using ChangeGear's Universal Data Services (UDS). This enhances the IT organization's ability to track and manage datacenter assets in a single integrated solution.

SunView Software Inc.

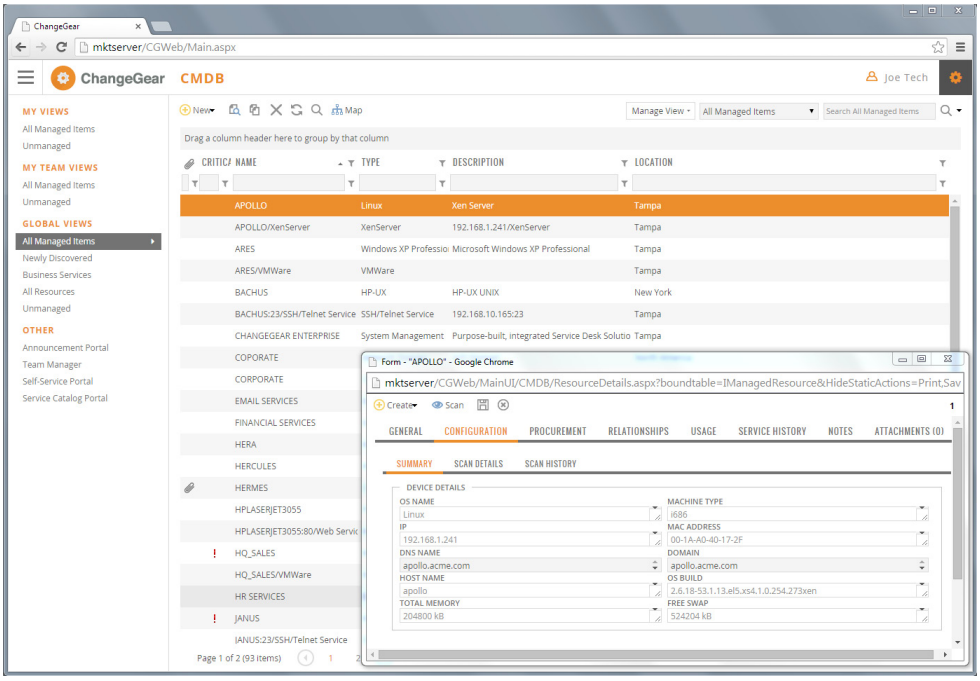
ChangeGear: A Complete Platform for Delivering Change & Configuration Management

ChangeGear is a web-based, best-of-breed Change and Configuration Management software solution that is easy to use and can be deployed quickly into your environment. Tightly integrating technology with process, ChangeGear simplifies change control and gives you the tools you need to track, manage, and control your critical infrastructure.

ChangeGear's extensible workflow is based on the Information Technology Infrastructure Library (ITIL) best practices framework out of the box. However, the workflow can be easily modified to fit your own internal processes - allowing your IT organization to define and automate the way you want to work.

In order to ensure IT controls are implemented, ChangeGear provides Change Management to make certain that every change introduced into the IT infrastructure follows a regulated process and Configuration Management for discovering, managing, and monitoring all of your critical assets.

Many features are included in the ChangeGear solution such as role-based security, auto-discovery of assets, workflow and business process automation, automated approvals and notifications, impact and risk analysis, historical audit-trails, and many more. Continue reading below for details on the features of functionality of ChangeGear, as related to complying with security regulations.



Are you a Government Organization?

Government organizations can purchase via SEWP or with our GSA Contract Holder. Our sales specialists can help you to understand what solution would best meet your needs and work with you through your purchasing process.

SunView Software Inc.