

Managing IT Risk and Compliance with CA GRC Manager

CA Governance, Risk & Compliance Manager (CA GRC Manager) helps to streamline and automate your IT compliance initiatives, improves your ability to manage and reduce IT risk, and increases your oversight of all your IT risk and compliance activities. It can help you significantly improve the effectiveness and efficiency of your IT GRC activities.

Overview	Benefits	The CA Advantage
Growing numbers of enterprises are struggling to meet increased regulatory requirements while also attempting to implement industry best practices and minimize an ever-increasing list of risks and exposures. And, their IT risk and compliance initiatives are complicated by the lack of a centralized, unified view of all IT risk and compliance information.	By providing a unified, enterprise view of IT risk and compliance, CA GRC Manager helps you streamline your compliance efforts, and improve visibility to emerging IT risks. The result is more timely and accurate information that enables you to make better risk-related decisions. In addition, it provides broad visibility into compliance project performance and the associated costs.	CA GRC Manager is a comprehensive solution that helps you manage your IT risk and compliance activities. It provides a centralized system to create and store business and regulatory policies, facilitate compliance with those policies, and manage the risks and costs associated with non-compliance.

The Challenge of IT Risk and Compliance

IT compliance executives today are faced with many challenges as they work to meet their compliance requirements. One of the most pervasive problems is the existence of compliance "silos", in which compliance information is maintained in separate locations across the organization. This can lead to a number of problems that are common today in most large organizations:

- The lack of centralized information about compliance programs, especially control status
- Difficulty in recognizing (and mitigating) emerging IT risk
- The inability to rationalize controls and to map them to various sections of the appropriate regulations

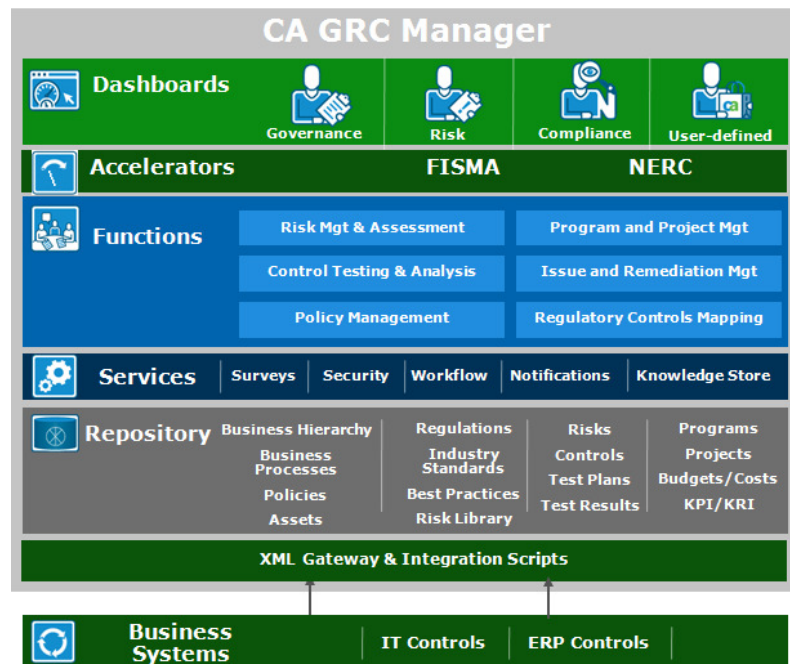
- The inability to measure and track compliance project progress
- The high costs of compliance and the inability to track those costs

The challenge of effectively managing IT compliance generally boils down to having excellent visibility across all your IT risks and controls, and being able to know and report on their current status. But, this has been an elusive goal due to the lack of centralized compliance information and the lack of automation that have plagued most organizations.

CA GRC Manager Improves IT Risk & Compliance

CA GRC Manager provides a unified, centralized view of compliance across your IT environment, allowing you to more effectively monitor and manage compliance controls and activities throughout your organization. It also increases your ability to manage IT risk, and to identify areas of emerging risk before they become critical. Finally, it improves the transparency and oversight of all of your IT risk and compliance initiatives.

The following graphic illustrates the broad capabilities of CA GRC Manager:



SINGLE GLOBAL REPOSITORY FOR COMPLIANCE CONTROLS AND RISKS

The CA GRC Manager global repository provides the foundation for your organization to continuously optimize processes for identifying risks and controls. This centralized repository can help to eliminate the silos of compliance and risk information that exist in many enterprises, greatly streamlining processes and improving decision making. The repository allows you to store information about specific risks and their mitigating controls and also relates the appropriate assets to those risks. And, detailed control information, such as test plans, testing results/evidence and remediation plans can also be associated with the controls.

With a global repository of policies, risks and control information that are mapped to relevant regulations, CA GRC Manager replaces the unsustainable mix of multiple systems and ad-hoc spreadsheets, charts and documents that are typically used to handle this

information. Because it helps unify multiple organizational silos, this approach provides executives with the information required to identify and manage reasonably anticipated risks and make better informed decisions about compliance costs, risks, benefits and action plans.

INTEGRATED, INDUSTRY-STANDARD FRAMEWORKS FOR CONTROL OPTIMIZATION

CA GRC Manager maps IT risks and controls to your corporate policies, as well as industry and legislative regulations and best practices. Thus, it optimizes your controls so you don't need to implement regulation-specific controls that drive up your compliance costs and create redundant effort.

To support this, CA GRC Manager incorporates the control and regulatory mappings provided by the Unified Compliance Framework (UCF), which includes more than 400 well-known standards and regulations, such as Sarbanes-Oxley (SOX), Basel II, the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), COBIT and the Payment Card Industry Standards (PCI), to help your organization optimize controls. In addition to the UCF, CA GRC Manager provides an extensible environment that allows for integration with internal or other third-party control frameworks.

By using CA GRC Manager to map regulatory requirements to a set of normalized controls, you can significantly reduce the total number of compliance controls you have to implement, support, and test. This, in turn, simplifies your compliance projects and can greatly reduce your total compliance costs.

COMPREHENSIVE POLICY MANAGEMENT

Policies can be the lifeblood of your compliance efforts. They help to ensure compliance with regulations and best practices, as well as enforce behavior and activity practices across the organization. Therefore, a robust policy management capability is essential for effective compliance management.

CA GRC Manager provides extensive policy management capabilities, including policy creation, communication, self-attestation and maintenance. CA GRC Manager helps you simplify and automate the entire policy lifecycle, which improves your visibility into the current level of adherence to all your compliance policies. And, by centralizing the management of your policies, you can help to establish consistency of policy format, communication, and enforcement across the enterprise.

DYNAMIC, REAL-TIME ANALYSIS OF RISK

CA GRC Manager provides extensive capabilities for the identification, evaluation, management and analysis of IT risk. Risk identification is aided through a large library of pre-defined enterprise risks that can be mapped to the specific business units, corporate business objectives or business processes that they impact.

Risk assessment can be automated through the use of user questionnaires and surveys, so that the process of gathering risk assessments is much simpler and less costly. In addition, automated assessments help to improve the timeliness and accuracy of your critical risk-related information.

CA GRC Manager's risk management capabilities enable you to create a *common IT risk management framework* across the organization. This ensures consistency of risk processes and helps to integrate effective IT risk management with your normal business processes. The result is higher quality risk information, and an increased ability to respond quickly to emerging IT risks.

In addition, CA GRC Manager supports key performance and risk indicators (KPIs, KRIs), including trend analysis of these key metrics. Risk Indicators can be created and defined for the unique needs of each environment, and then tracked on an ongoing basis. These

metrics help enable more precise evaluation of the current risk profile so that more informed decisions can be made for risk mitigation.

ROLE-BASED DASHBOARDS THAT STREAMLINE DECISION MAKING

CA GRC Manager includes a large number of pre-defined user roles (e.g., Compliance Manager, Controls Tester, IT Risk Manager, etc) that include pre-configured dashboards and reports. These extensive pre-configured templates provide the information that each person needs, in a format best suited to their individual preferences and roles. This helps to improve visibility into your current risk profile, streamline decision making, and help ensure rapid issue remediation.

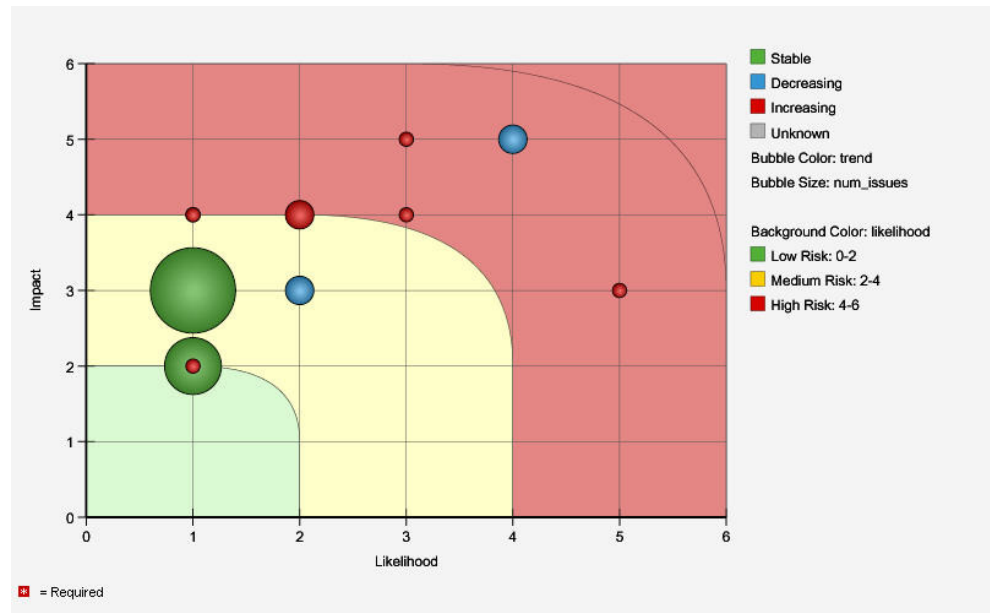
These role-based views can be configured to meet the specific visualization needs of your organization and your individual users, helping you manage data from an executive’s point of view down to a more detailed level. Specifically, CA GRC Manager includes a suite of pre-defined dashboards, including:

- Regulatory Controls
- Performance Trends
- IT Risk
- Control Status
- Test Results
- Additional dashboards that can be easily included without requiring customization

Moreover, more than 25 drill-down portlets are pre-defined to provide more granular detail regarding dashboard data.

EXAMPLE OF ROLE-BASED RISK DASHBOARDS

FIGURE C



INTEGRATED PROGRAM AND RESOURCE MANAGEMENT CAPABILITIES

Many companies are challenged by poor remediation project execution, lack of visibility into their current status, and escalating and untracked project costs. CA GRC Manager includes

rich compliance program and project management capabilities to ensure that optimal compliance remediation plans are produced, communication barriers are eliminated and compliance projects are executed effectively. Moreover, GRC Manager supports any level of project planning — from simple to sophisticated.

Managers responsible for remediation projects can easily create simple plans for collaboration and the tracking of key tasks and milestones or detailed plans for capturing all of the information in a complex program. Collaboration is a basic element in every plan and includes threaded discussions and document management, as well as time tracking at the project or task level. Plans can also include key tasks, Work Breakdown Structure (WBS) hierarchies, estimates, dependencies and deliverables and staff assignments. Finally, all project resource and cost accounting activities are fully integrated, allowing for seamless management throughout the project life cycle.

With integrated resource management capabilities, CA GRC Manager offers an aggregated and summarized view of the labor and non-labor resources associated with controls implementation, testing, remediation and risk assessment across the organization, enabling you to better optimize the personnel and costs of managing compliance initiatives. And, these resource administration and coordination capabilities provide a solution to plan and manage resource capacity and balance it against work demand — a required component of any remediation or audit project.

INCREASED VISIBILITY INTO THE COST OF COMPLIANCE PROGRAMS

Most importantly, CA GRC Manager can capture and track the costs of all your remediation projects. In this way, CA GRC Manager can provide visibility into the cost of compliance and deliver the financial management tools you need to accurately capture expenditures, access historic information and generate a wide range of financial reports. This visibility can help you eliminate the “hidden costs” of compliance that plague so many enterprises.

COMPLIANCE ACCELERATORS FOR SPECIFIC REGULATIONS

CA GRC Manager includes Accelerators for NERC and FISMA, with several other Accelerators under development. These add-on components consist of content and frameworks that are specific to a given regulation and can greatly simplify the process of compliance with the regulation, lower your time-to-value, and reduce your overall compliance costs.

FLEXIBLE PLATFORM OF COMMON SERVICES

CA GRC Manager is a pure J2EE web-based application, and as such, all of its capabilities are supported by a set of core services, including collaboration, document management, reporting and analytics, in addition to a portal-based framework. Underlying this is a proven architecture that offers unmatched scalability, high availability and broad platform support.

KEY CONTROLS AND BUSINESS SYSTEMS OF RECORD INTEGRATION

CA GRC Manager integrates with a variety of automated controls mechanisms. In particular, business systems of record can be integrated using the XOG™ (XML Open Gateway) service, a comprehensive set of eXtensible Markup Language (XML) and Java-based APIs. To ensure consistency and reliability, XOG preserves data integrity through the enforcement of business rules and information exchange through integration APIs that access the same business logic as when a user manually enters data.

CA Services

Augmenting CA GRC Manager’s product capabilities, the CA Services team offers a variety of customized services to help ensure the successful implementation and use of CA GRC Manager. In addition, CA works closely with leading Global System Integrators for delivery of GRC services, which can include:

- Implementation planning and delivery services
- Migration and upgrade services
- Post-implementation business analysis

CA GRC Manager replaces the unsustainable mix of multiple systems and ad-hoc spreadsheets, charts and documents that are typically used to handle policies, risks and control information.

Improving the Overall Management of IT Risk & Compliance

The ability to establish sophisticated evaluation and selection criteria, create and optimize risk planning scenarios, communicate decisions and monitor compliance progress in a seamless, integrated system makes CA GRC Manager a critical tool for helping to manage IT risk and compliance efforts throughout your organization.

Centralization of IT risk and compliance information helps to improve your risk-based decisions, and to simplify your key compliance processes. Role-based and customizable dashboards streamline decision making and help ensure rapid issue resolution through a consolidated view into the monitoring, management and reporting of your compliance controls.

And rich program management capabilities help ensure that compliance projects are executed successfully, while tracking compliance costs across all your compliance initiatives.

As such, CA GRC Manager can help you:

- Simplify and automate your key compliance processes
- Improve decision making and oversight of your compliance controls portfolio
- Eliminate redundant compliance controls using industry-standard frameworks and regulation mappings
- Improve the visibility to your total IT risk profile, and ensure effective risk mitigation
- Improve transparency and the overall oversight of your IT risk and compliance initiatives

The CA Advantage

CA GRC Manager is an integral component of CA's IT GRC solution, which can help your organization manage risk through a unified approach that incorporates the automation and continuous monitoring of the broadest set of underlying IT controls, including those for Security Management, Information Management and Change and Configuration Management.

CA GRC Manager delivers a unified, IT-wide view of risks and compliance. These capabilities help to ensure that exposures are identified so that management can make informed decisions about compliance costs, risks, benefits and action plans.

Next Steps

If you're finding that:

- You are managing IT risk and compliance activities in different silos, with duplicated information spread across the organization
- You are duplicating efforts across all your compliance programs
- You need to increase the automation of your controls for greater efficiency
- You lack adequate visibility into the current state of your IT risk
- You don't have an effective way to track the progress and total costs of your compliance and remediation projects

Then take a look at CA GRC Manager. It can help you improve the management of IT compliance and risk across your organization and eliminate your existing silos of compliance information and activities.

To learn more, and see how CA software solutions enable other organizations to unify and simplify IT management for better business results, visit ca.com/customers.

Copyright © 2009 CA. All rights reserved. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies. This document is for your informational purposes only. To the extent permitted by applicable law, CA provides this document "As Is" without warranty of any kind, including, without limitation, any implied warranties of merchantability or fitness for a particular purpose, or non-infringement. In no event will CA be liable for any loss or damage, direct or indirect, from the use of this document including, without limitation, lost profits, business interruption, goodwill or lost data, even if CA is expressly advised of the possibility of such damages. CA does not provide legal advice. Neither this document nor any software product referenced herein shall serve as a substitute for the reader's compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, standard, policy, administrative order, executive order, etc. (collectively, "Laws")) referenced herein. The reader should consult with competent legal counsel regarding any such Laws.