Agiliance®

Continuous Compliance: A Better, Faster, Cheaper Way to Comply

Business White Paper

TABLE OF CONTENTS

Executive Summary

Businesses today are under increased pressure to cut costs, optimize performance and reduce risk. The need to meet these challenges is particularly apparent in the area of regulatory compliance. Historically, businesses responded to emerging regulatory requirements by assigning a dedicated compliance team to handle every new mandate, each with its own specific team, mission and project scope. But as regulations continue to proliferate and evolve, this approach is directly at odds with business requirements to improve performance, reduce costs and more effectively manage risk.

Dedicating a new team to each regulation is not an effective use of resources at a time when "do more with less" is re-emerging as the mantra of the day. The costs of this approach are substantial, both in terms of the direct cost of resources and the impact on IT, which finds itself deprived of the resources to handle core responsibilities – because those resources are increasingly consumed by compliance related projects. But what is the alternative, given the amount of effort required to manage compliance in a rapidly changing and increasingly complex regulatory landscape?

By automating current IT compliance processes already in place, business can significantly reduce costs and increase operational efficiency – reducing the resources required to address compliance and returning IT resources to core business priorities. An automated approach to compliance can improve data consistency through aggregation and enable a state of continuous compliance, in which it's possible to tell the status of a company's compliance at any given time and without additional effort. Continuous compliance reduces risk by providing visibility into compliance related issues and remediation efforts across the organization to ensure confidence in the company's current compliance status prior to an IT audit or under any other circumstances.

Today, companies are beginning to demonstrate measurable success in adopting processes that are characteristic of continuous compliance, as part of a larger implementation of IT governance, risk and compliance practices. Network World recently reported on a study by the IT Policy Compliance Group which showed that companies with the most mature IT GRC practices tended to have the best business results, including higher revenues and profits and much lower spending on regulatory audits – 50% lower ("IT governance best practices are critical for business success," 11/21/08).

This paper examines in greater depth the need for continuous compliance, describes how automation enables continuous compliance and explores the cost saving benefits and operational benefits of an approach that aims to achieve a state of constant, uninterrupted compliance. It includes a detailed discussion of specific compliance-related processes that companies can automate to improve the effectiveness of compliance programs and cut costs, as well as a forward-looking discussion of how continuous compliance can better position companies to move toward better overall risk management.

The Evolution From Reactive Compliance to Continuous Compliance

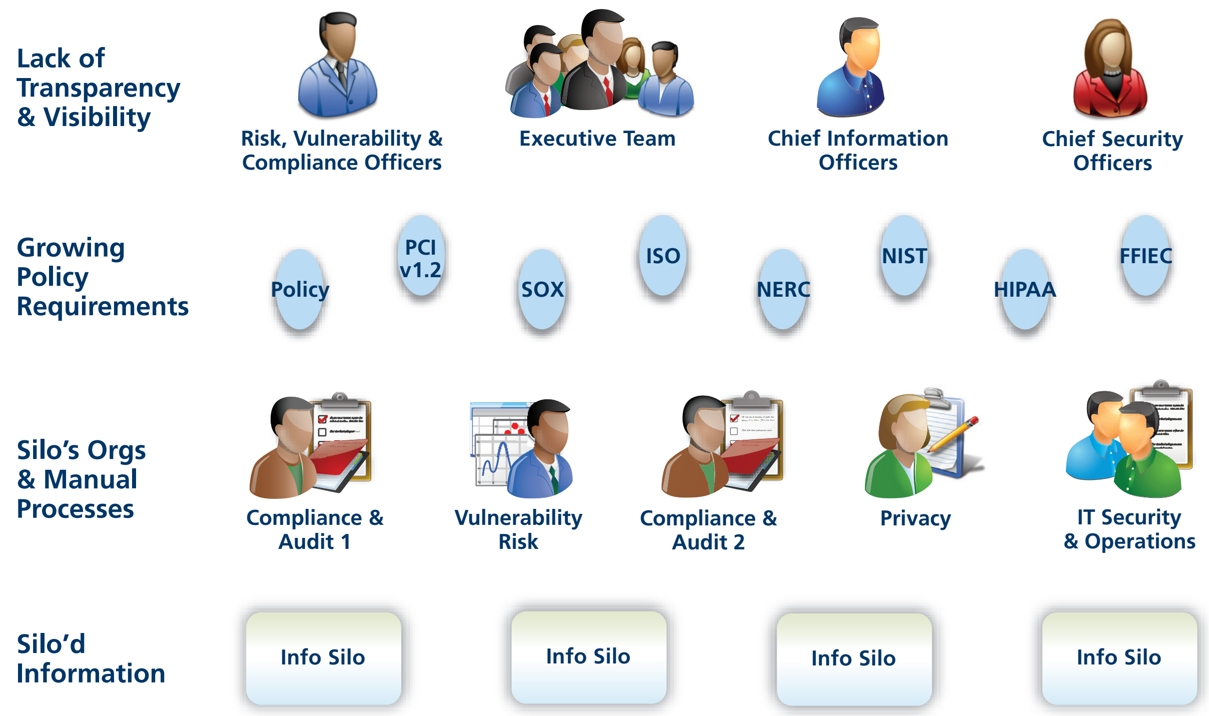
Continuous compliance can be defined as a company's ability to be in compliance – or at least to know whether it is in compliance, and how to respond if it is not – at all times, across all operations. For any company under the burden of multiple regulations, or under significant operating burdens from a single industry-specific regulation, continuous compliance is essential. It is the next logical stage in the evolution of compliance.

First Stage: Reactive

As regulatory activity began to increase in the mid-2000s, businesses generally responded by assigning a team to address each new regulation. The team would set policies, establish controls and perform assessments; when the next regulation was announced, a new team would follow suit. This is still the way many companies approach compliance today. There is nothing inherently wrong with the policies-controls-assessments paradigm, but there are several weaknesses in its original form.

1. *It is very expensive.* Assessments, control testing and reporting are largely manual, fragmented efforts. As a consequence, this approach does not take into account the significant amount of overlap among

The Business Challenges Associated with a Reactive Approach to Compliance



different regulatory requirements and it misses the opportunity to increase efficiency by automating the manual processes and reduce costs by leveraging existing work and controls across all regulations.

2. *It is by definition reactive rather than proactive,* making it difficult to get far enough ahead of the game to establish and maintain a state of constant compliance.

3. *Transparency into risk is never achieved.* In the siloed and fragmented approach, multiple teams of people, often from multiple operational perspectives, are tackling multiple regulations and audits. This makes it impossible for executives who are ultimately responsible for certifying a company's compliance to have the broad visibility into compliance that they need to confidently sign off on its status.

Next Stage: Proactive

Continuous compliance is the next natural step in the evolution of compliance practices. It builds on existing processes and paradigms by enabling a proactive approach that improves compliance by making it a constant state. Continuous compliance addresses the weaknesses inherent in a reactive approach to compliance on several levels.

1. *It uses automation to efficiently correlate requirements* among different regulations and address them in concert, which lowers costs by eliminating unnecessary redundancy and repetition. Costs are also significantly reduced by automating what were manual, labor intensive tasks.

2. *It is not disruptive* and requires no sudden and costly outpouring of resources every time a new regulation is introduced.

3. *It delivers transparency* by providing current and accurate visibility into the monitoring, management and reporting of risks and controls across the entire organization. This reduces business risk by putting executives in a position to know the company's compliance status, and to track progress of remediation efforts, with certainty and to sign off on compliance reports with confidence in their accuracy.

> Based on Agiliance's experience with its own clients, companies can reduce the cost to achieve compliance by 80-90%.

Making the Transition

More and more companies today are moving toward proactive, continuous compliance. To do this, they are building on existing compliance programs by automating the processes already in use. Approaching the transition as an overlay to existing processes helps reduce the cost of and time to compliance and makes it possible to quickly achieve time to value. Based on Agiliance's experience with its own clients, companies can reduce the cost to achieve compliance by 80-90%.

Compliance Automation: The Key to Continuous Compliance

Compliance automation involves automating the processes associated with achieving and maintaining compliance. It improves on existing projects and efforts by introducing automated and repeatable processes and workflows to compliance programs. The greatest benefits are achieved when company affects this shift to automation at all points in the compliance lifecycle:

- Continuous compliance depends upon a company's ability to *aggregate and correlate* information from across the organization in order to determine the degree of compliance risk and create the policies to address it. Without automation, there is no single, simple, streamlined way to do this, given the multiple, manual efforts that are likely to be underway at any given time.

- Once the degree of risk and the policies to address that risk have been determined, automation can be used to help *monitor and control* the IT environment, or to put measures in place that make it possible to monitor compliance and remediate problems. Without automation, there is no way to do this in an accurate, repeatable, timely, or cost-effective manner.

- Finally, automation is invaluable in the ongoing effort to *analyze and remediate*, and to institute ways of measuring, reporting on and documenting compliance and remediation. Automation enables the accuracy and predictability that are essential to the effectiveness of such metrics.

Introducing automation into efforts to define, control and govern the IT environment enables companies to reduce costs and improve compliance by:

- *Reducing the operational expense* associated with manual processes across multiple, fragmented teams working independently, including the costs associated with consultant teams brought in to perform assessments and produce reports;

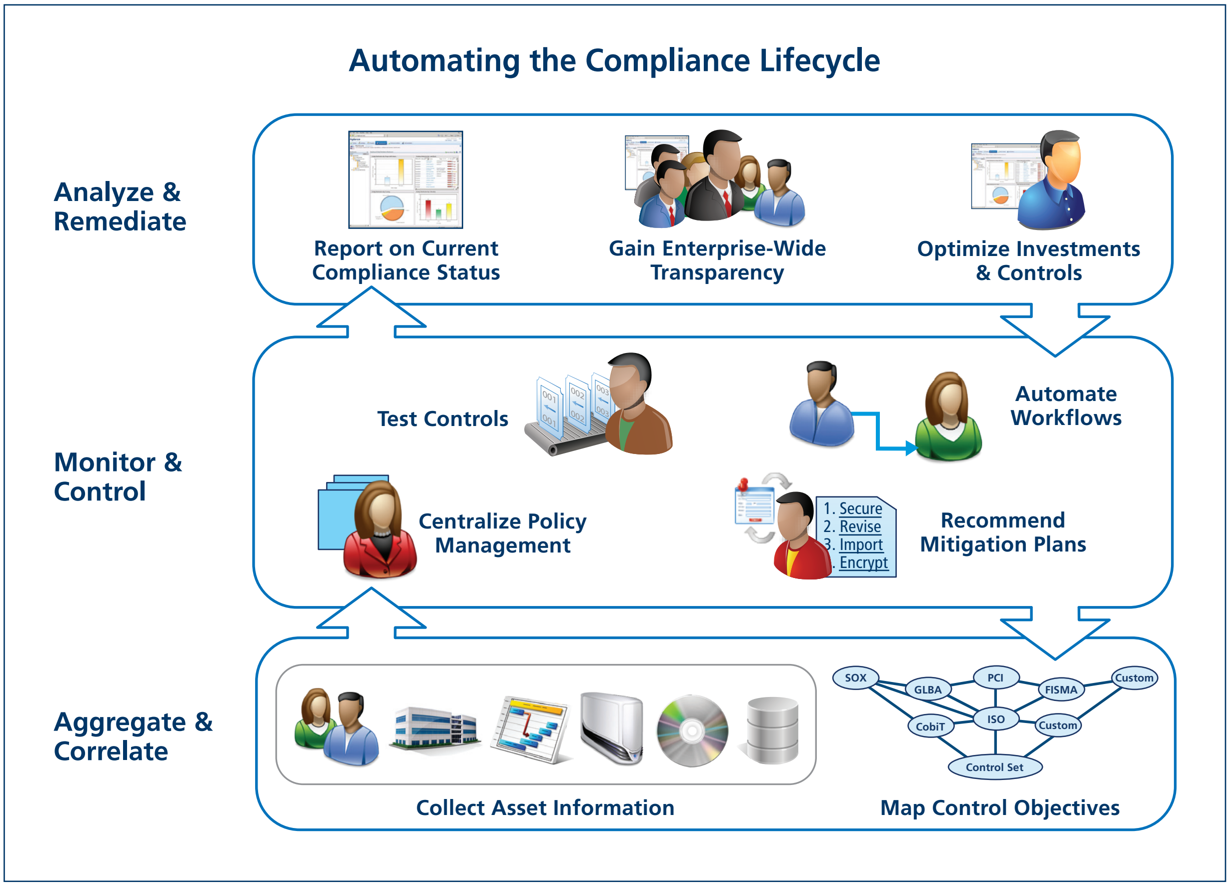
- *Achieving the high level of accuracy and consistency* that results from bringing together independent, inconsistent silos of information and eliminating error-prone manual processes for working with the information in them;

- *Providing transparency across the board* into current compliance and risk status – organized by division, business process, system, or whatever is required at any given instance – and providing ongoing metrics and reporting.

> The result is the ability to be confident in and be able to demonstrate, compliance status at any given time – with minimal effort and at a much lower cost. In addition to these direct benefits, compliance automation also enables companies to reallocate budget and resources to more productive, strategic activities that are forward looking to revenue generation and competitive differentiation.

Compliance Automation in Action

In the abstract, it’s easy to discuss the idea of automating compliance processes. But exploring specific examples makes the value of compliance automation and continuous compliance more apparent.



Automating the Compliance Lifecycle

Aggregate and Correlate

SOX
GLBA
PCI
FISMA
Custom
CobiT
ISO
Custom
Control Set
Collect Asset Information
Map Control Objectives

Why automate?

Among the most time-consuming and costly activities associated with assessing compliance risk and establishing policies to enable compliance is the seemingly simple act of collecting and organizing relevant information from IT systems. Doing this manually means dedicating significant human resources to checking scanners, CMDB’s, directories, identity management repositories and other sources of information to determine whether controls are passing or failing. It is also difficult to mount any sort of streamlined, coordinated effort without any centralized oversight. Additionally, testing controls often requires the execution of surveys to gather information from employees, partners and vendors, which is also a manual, fragmented and expensive effort, that relies heavily on email, spreadsheets and paper-based processes.

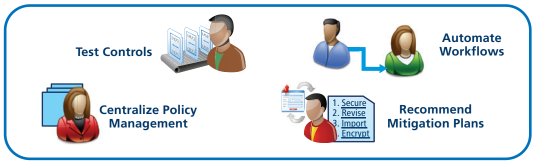
There is a similar problem today with the effort to identify the specific requirements of regulations and create strategies to meet them. For example, if a company has to comply with Sarbanes-Oxley and Payment Card Industry (PCI) requirements, and also wants to be ISO-compliant, a team will be assigned to each regulation or standard to identify its requirements and define the appropriate controls to implement. But more often than not, there is considerable overlap in requirements. Mapping these requirements to each other helps reduce the number of people and teams dedicated to compliance efforts. If the mapping itself is done manually, that activity will still consume considerable resources.

How to automate?

Compliance automation makes it possible to collect and classify information from across the enterprise in a concerted, automated effort. This dramatically speeds efforts to reconcile data from geographically or technologically diverse systems, classify information from those systems and identify areas of concern that can be corrected before they become issues in an audit. Surveys can be conducted leveraging web-based interfaces and workflow to gain further efficiencies.

Compliance automation also provides companies with a pre-mapped framework that spans across regulations, frameworks, standards and policies and maps controls to the people, processes and IT assets that are affected by them. With this, automated assessments and reporting can quickly be put in place.

Monitor and Control



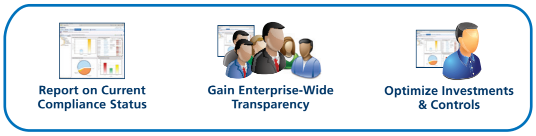
Why automate?

Testing controls to determine whether they're working (and to decide what can be done if they're not) generally requires asking people about the application of the control and documenting their responses. But doing this manually is rife with potential problems. It is not only costly and time-consuming, it's subject to error. For example, suppose you want to test password policy by determining whether passwords are being changed on the basis set forth by the policy. Asking people if they changed their password in the last month doesn't guarantee that their answers will be accurate. They may have forgotten or they may just not want to admit a failure to comply.

How to automate?

Using automation to test controls speeds the process and helps ensure accurate responses. When someone uses an automated system to gather password change information from systems, for example, the information that is collected is going to reflect what actually happened. Either the password was changed or it wasn't, which is preferable to relying on a user's memory – which may or may not be accurate. Compliance automation makes it possible to definitively detect failure, recommend remedial action and automatically recheck to be sure that the problem is resolved.

Analyze and Remediate


Report on Current Compliance Status
Gain Enterprise-Wide Transparency
Optimize Investments & Controls

Why automate?

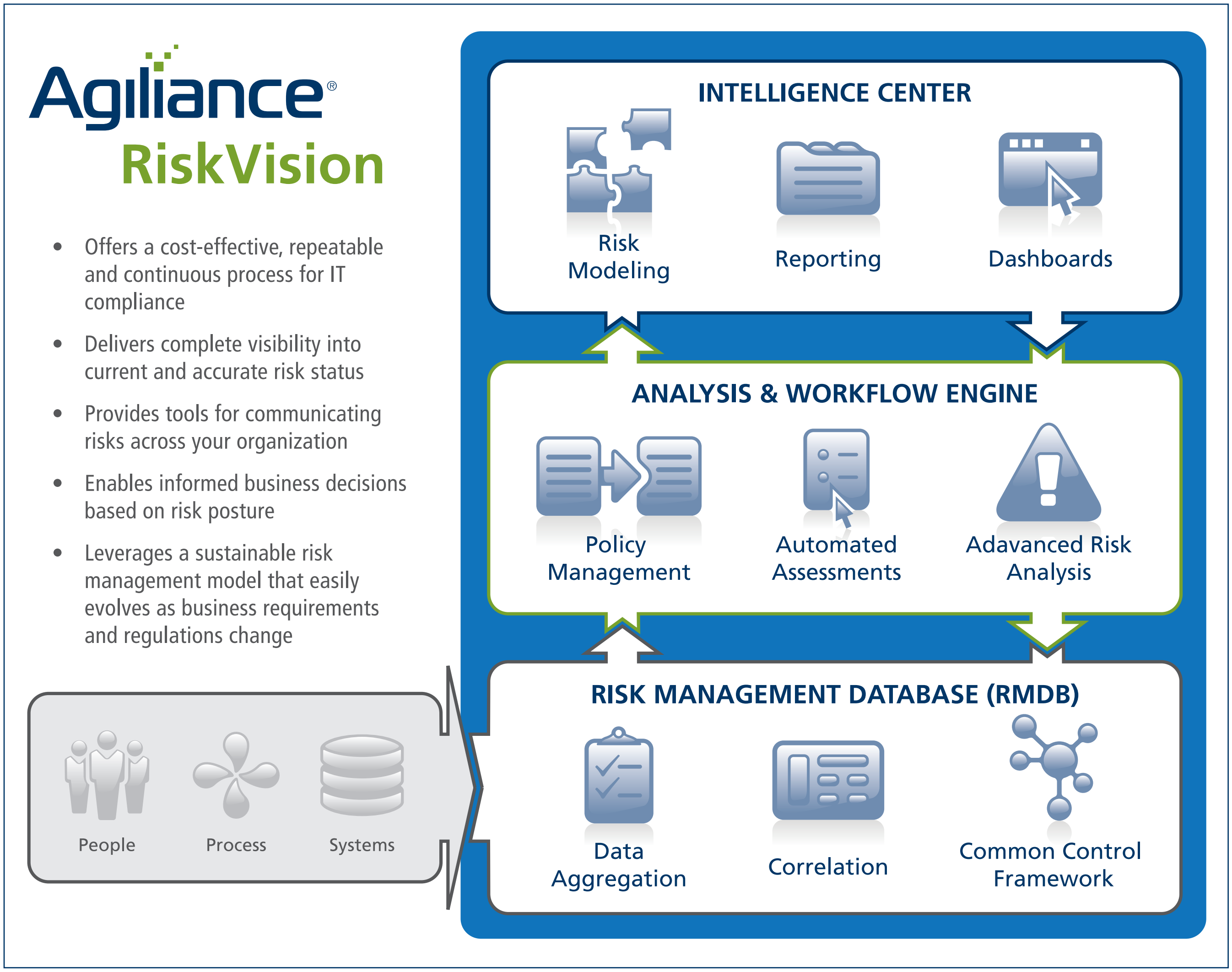
Governance, in the context of compliance, means providing the oversight to ensure over the long term that a company's compliance-related policies, processes and controls are actually working. In the non-automated environment, companies tend to focus on ensuring that the right security policies and technologies are in place, but not necessarily on validating that the measures that have been implemented are actually working and that there is visibility into that effectiveness. Shoring up the latter is essential to managing overall business risk, not just compliance risk.

How to automate?

Compliance automation answers the critical questions surrounding compliance and risk: Are our security policies effective? Are the controls which we have put in place working – are they making us more secure? If not, why not? And how can we fix it? Compliance automation achieves this by providing the infrastructure needed to deliver consistent, centralized visibility into information related to risk and compliance. It allows a company to apply enterprisewide standards to risk- and compliance-related activities, measuring their effectiveness, reporting on it, tracking trends and maintaining a record of this information. In this state of continuous compliance, a company can easily demonstrate compliance status at any time.

How Agiliance Can Help

Agiliance can help dramatically reduce the time and costs associated with managing compliance while improving the ability to comply, by automating manual activities and enabling continuous compliance. Using Agiliance RiskVision™, companies can gather data from systems, applications, people and processes with far less effort than doing so manually. Agiliance also enables companies to automatically assign controls and continually monitor them across a variety of regulations, standards and policies, providing complete visibility into an organization's compliance status at any time.



Agiliance® RiskVision

- Offers a cost-effective, repeatable and continuous process for IT compliance
- Delivers complete visibility into current and accurate risk status
- Provides tools for communicating risks across your organization
- Enables informed business decisions based on risk posture
- Leverages a sustainable risk management model that easily evolves as business requirements and regulations change

Capabilities

Aggregate and Correlate

- Provides a single authoritative source of IT risk
- Aggregates non-IT entity data (e.g., people, vendors and processes)
- Aggregates IT entity data (e.g., servers, applications and network devices)
- Provides a common control framework to streamline efforts across multiple regulations and best practices

Monitor and Control

- Delivers centralized policy management
- Automates control monitoring, testing and reporting
- Provides a complete, closed loop risk management system

Analyze and Remediate

- Provides executives with up-to-date risk and compliance status
- Offers granular insight and analytics to explore risks and prioritize remediation
- Delivers dynamic risk modeling to support ongoing risk management
- Provides advanced workflow for streamlining remediation efforts
- Measures the effectiveness of compliance and risk initiatives

REAL RESULTS:

A Fortune 500 grocery chain lowered compliance costs by over 90% using Agiliance RiskVision.

- Three fulltime consultants were brought in to conduct compliance assessments for Sarbanes-Oxley, PCI and COBIT.
- This team was conducting manual control tests on 250 IT assets (servers, scanners, etc.) with 1,200 control checks executed quarterly, and 500,000 control checks executed annually.
- Executive management was seeking a consolidated view of the status of compliance with Sarbanes-Oxley and COBIT, so the consultants were hired to create quarterly reports from the result of the manual control checks.
- This effort was costing the company over $1.5 million per year.
- By implementing RiskVision, they were able to save over 90% of the spend, because the current state requires only one half-time employee to manage the entire process.

REAL RESULTS:

A $2.2 billion ecommerce company cut its time to compliance in half and saved 80% annually in consulting fees using Agiliance RiskVision.

- The company's regulatory requirements included adherence to Payment Card Industry (PCI), the European version of Sarbanes-Oxley, and to the EU Data Protection Directive.
- The compliance team was managing an infrastructure of more than 2,000 IT assets (servers, operating systems and applications, network devices).
- Security and IT managers were over burdened with the task of manually monitoring risk data from IT systems such as vulnerability scanners and security incident managers and mapping results from surveys stored in word documents, spreadsheets and email chains.
- The aggregated information from risk monitoring was manually mapped to regulations to assess the relative degree of compliance – a very costly and time-consuming process.
- By implementing RiskVision, the company was able to cut time to compliance by 50%, reduce unplanned consulting service costs by 80% and significantly reduce staffing requirements and unplanned implementation fees.

Benefits

Reduce compliance costs by automating data collection and control testing

Agiliance software connects with a wide range of IT and security infrastructure assets and enables extensive web-based self-assessments with the ability to import findings. In addition, automated workflow provides repeatable assessment processes, including advanced remediation and mitigation. The software automatically aggregates and correlates data across systems, people and processes. Control tests and assessments that today are done manually by teams of staff or consultants can be done in an automated, repeatable fashion.

Lower costs and increase efficiency by mapping multiple regulatory requirements

Agiliance software pre-maps controls across a wide range of regulations, standards and frameworks; companies can select relevant regulations, policies, security threats and frameworks and be ready to test controls in minutes. As regulations evolve and new assets are added to the infrastructure, the software automatically updates controls to reflect changes.

Streamline compliance by eliminating testing redundancies

Agiliance software eliminates duplicate testing across multiple regulations and speeds up the time to compliance. Using the built-in Common Control Framework, which contains over 10,000 controls over a broad range of authoritative sources, companies can test a control one time to satisfy requirements that are common to multiple regulations. This eliminates the time and cost associated with duplicate testing of controls.

Manage remediation and exceptions more efficiently

Agiliance software automatically prioritizes IT assets that need to be monitored so that the most critical assets – those containing personal information, medical records or credit card data, for example – can be addressed first. Managers can immediately view the cost of asset downtime, impact of risk mitigation plans and cost of asset replacement, so they can make real-time decisions about remediation. Decision makers can use this data to make more-informed decisions about allocating budget toward critical assets.

Proactively manage risk

Agiliance software includes advanced modeling capabilities that allow analysts to view the cost of controls, vary the level of controls applied and assess changes in risk values before proceeding to implement controls. For example, if unencrypted data on a server violates established controls, the modeling capabilities make it possible to calculate the cost for remediation as well the cost associated with the risk exposure. If the former is greater, an informed choice may be made to issue an exception rather than proceed with remediation.

Provide complete visibility into current status with ongoing metrics and reporting

Agiliance software provides decision makers with current and accurate intelligence on risk and compliance status. Role-based dashboards and pre-configured report templates provide tailored views. Reports can be delivered to executives, managers or security analysts, with details presented by division, regulation, business process or other customizable views. Companies can rely on Agiliance to deliver continuous monitoring of risk and compliance across the enterprise.

> *“Not only did the Agiliance solution alleviate some immediate pain through automation of the seemingly never-ending list of compliance assessments, I believe it will ultimately help us implement a proactive and cost effective risk management strategy.”*
>
> **– Shane Fuller**
> **Information Security & Compliance Manager**
> **RSA Insurance**

Why Agiliance

As the costs and complexity of IT risk and compliance management continues to rise, Agiliance believes that customers deserve high performance solutions that completely address the IT risk and compliance demands of today and scale to meet future challenges. Agiliance RiskVision was built from the ground up as an integrated IT risk and compliance management platform that supports the automation and risk intelligence requirements of today's enterprise. Agiliance solutions are highly configurable and easy to integrate so that companies can realize time to value in 45 days or less.

Our security automation and enterprise software acumen allows us to offer the capabilities to support long-term risk management goals and to realize 80-90% reduction in compliance related costs, based on our experience with customers to date. By offering market-ready "quick-start" solutions, Agiliance helps companies progress from first phase compliance projects through to robust and strategic IT risk management programs with ease and confidence.

With the industry's most powerful risk management and automation platform, Agiliance is the company that the Global 2000 trust to solve their most pressing risk issues including business continuity management, vendor risk management and compliance management.

ABOUT AGILIANCE

Agiliance offers highly automated IT risk and compliance management software products designed to help organizations thrive in the face of mounting pressures to manage and balance risk, compliance and IT budgets. Global 2000 companies in the financial, healthcare, energy, government and technology industries are leveraging the power of Agiliance software to cut compliance costs and to provide decision makers with the current and accurate intelligence they need to better understand how IT risk affects their entire organization.

Agiliance, Inc.

2001 Gateway Place,
Suite 315 West
San Jose, CA 95110

p: 408.200.0400
f: 408.200.0401
www.agiliance.com

© 2008 Agiliance, Inc.
All rights reserved.