



The Leader in Integrated Governance, Risk, and Compliance

**SOLUTION BRIEF**

Federal Government IT Enterprise Risk Management

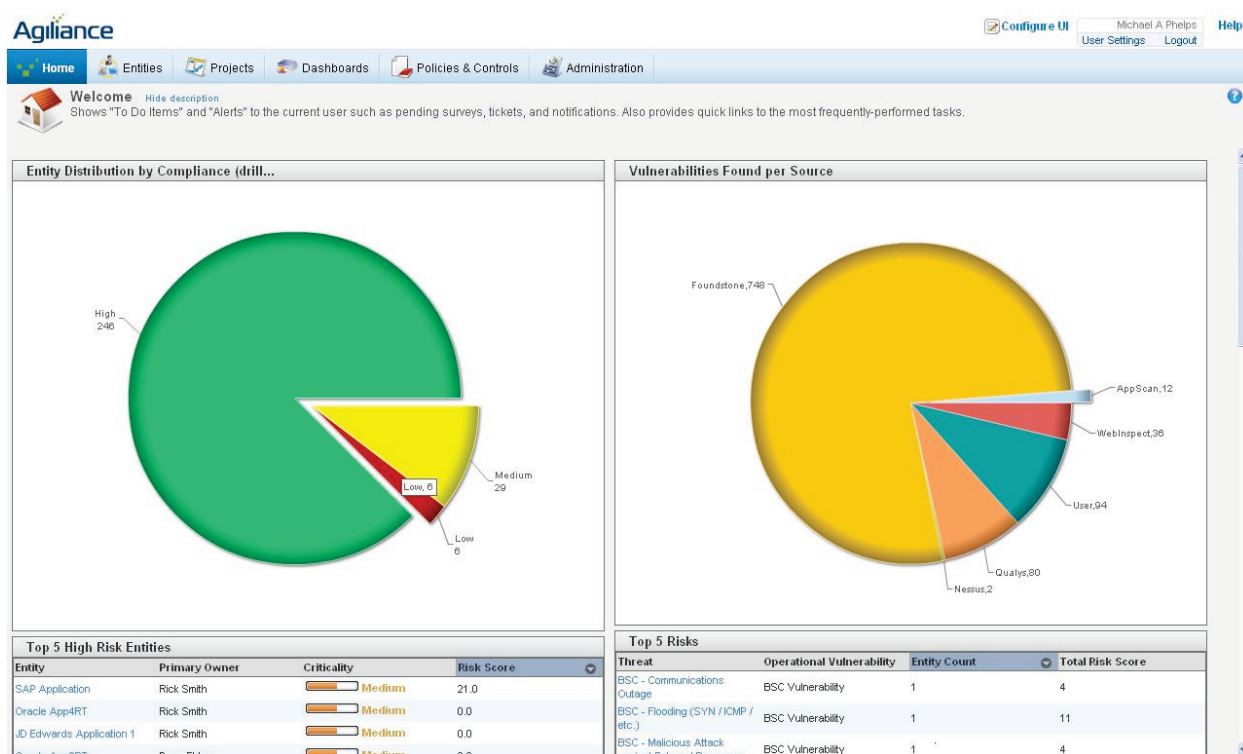
# **Achieving Organizational Maturity through Risk and Compliance Automation**

# Table of Contents

The Risk and Security Operational Picture .....	3
Enterprise Risk – The Challenge.....	3
Solution.....	4
Identify Risk .....	4
Create Ongoing Risk Assessments .....	5
Integrate and Automate Technical Controls.....	5
Demonstrate Continuous Regulatory Compliance .....	5
Manage risk .....	6
Track Enterprise Risk Trends.....	7
Conclusion .....	7
About Agilience.....	7

## The Risk and Security Operational Picture

Federal agencies can achieve superior performance when managing risk proactively. By anticipating future security risks and taking steps to alleviate negative outcomes, agency management can be reasonably sure that they will meet organization’s policy objectives. The standards-based Agilience Governance Risk and Compliance (GRC) Solution enables agencies to holistically manage all enterprise risk - both IT and non-IT making it a comprehensive solution. The Agilience GRC Solution uniquely incorporates methodologies to address current, future and historical risk trending.



Custom dashboards arm line-of-business executives with the knowledge to act on risk that has a direct impact to the organization. Agilience provides a highly flexible security and risk dashboard tailored to the mission priorities and objectives of the organization, which can be shared across the executive management team to facilitate risk prioritization and obtain a real time situational awareness of the organization’s risk and security posture.

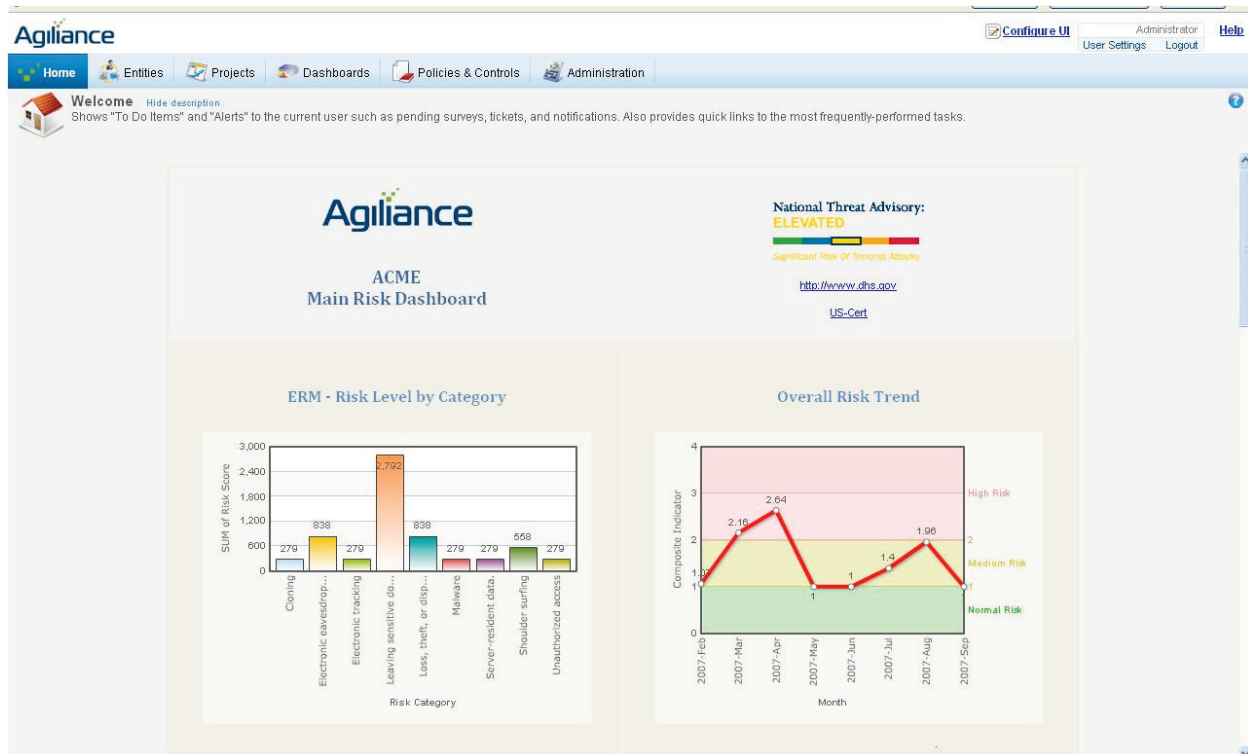
## Enterprise Risk – The Challenge

New congressional contracting protocols, budget cuts and increase in regulations stipulate that any major new agency programs will be required to identify areas of risk management, show that the technologies required for the program have been proven in lab tests, and prove that the project complies with department regulations. Enterprise risk management empowers managers to identify and analyze the many risks that can affect the organization. Identifying preventive steps reduces the likelihood and magnitude of adverse impacts. The challenge most organizations face is that they must determine how to measure and manage risk consistently and sustainably, given its highly subjective nature and its reach into many disparate areas of the organization.

## The Solution

### Identify Risk

Agilience follows leading standards body guidance, including COSO ERM and AS/NZ 4360, while also accommodating custom risk statements. It enables organizations to easily aggregate risk information, collaborate in risk and response decisions, and ensure the follow-through required to manage risk.



With Agilience, organizations can establish a single risk score for all applicable risks, spanning from business to IT.

In addition, organizations can benefit from the entire Agilience RiskVision™ GRC platform to automate the entire ERM process and workflow, from scoring to mitigation and reporting. Aggregate risk-score status alerts provide timely, actionable information backed by audit trails and reporting visible to executive management and the board of directors.

Agency leadership must make better, more informed, timely business decisions based on objective, risk-based information in support of strategic business goals. With Agilience, organizations proactively address risks, whether doing so is mandated by regulators or recognized as a strategic imperative in an increasingly uncertain world.

## Create Ongoing Risk Assessments

Commonly, technology risk assessments and compliance testing use manual processes, questionnaire driven personal interviews. The tools are e-mail, paper and spreadsheets.

These manual processes and tools are difficult to manage and prone to error. They are costly, time consuming, confusing and complex. Results become obsolete because manual testing per regulation is typically done only once a year and it is impractical to share results across regulations.

The Agilience integrated RiskVision GRC platform automates the survey process to increase the quality and timeliness of controls testing while simplifying the effort and lowering the cost. Agilience not only automates the survey workflow but also provides the content necessary to build surveys, which is essential.

Survey process automation used with a common control framework and asset repository can dramatically reduce errors, increase response quality, and cut the time to complete the survey work.

These benefits accrue to all involved, including project managers, respondents, auditors, and executive management, allowing an increase in survey frequency for a nominal cost.

## Integrate and Automate Technical Controls

Computing assets, hardware, software, and other IT assets, are generally subject to technical controls that can be monitored automatically. Automated testing can be performed frequently, even continuously.

Agilience RiskVision easily integrates with already deployed systems such as scanners like Nessus and other monitoring systems like ArcSight SIEM. The solution connects remotely without the use of an agent running on the servers or hosts to avoid the complexity and cost of managing hosted agents on large numbers of servers.

Full automation, while desired, is not always easy to achieve. Many objectives depend on controls that involve a combination of manual or procedural as well as technical checks. However, Agilience supports both automated survey workflow and technical testing seamlessly combining the data from each resulting in a comprehensive view of risk and compliance. By combining the results of both technical and procedural controls testing, the organization achieves a compliance and risk picture that is more complete, accurate, and up-to-date as well as less costly to develop.

## Demonstrate Continuous Regulatory Compliance

Today, most regulations are managed independently. Because of the extensive overlap among regulatory policies, and therefore in policy controls, this approach is cumbersome and redundant. It is also complex and expensive.

While some organizations maintain custom control sets, others have been able to take advantage of standard frameworks such as COBIT, NIST SP-800-53, and ISO 27002. In some cases, organizations apply a specific standard control framework to a specific regulation. Examples are NIST 800-37 for Certification and Accreditation, NIST 800-66 for HIPAA and COBIT for OMB A123. In others, they apply a mix of standards-based and custom controls. Using standard frameworks has aided organizations by reducing the overhead required to develop and maintain custom controls.

However, there is still more benefit to realize. A significant number of specific control requirements are common across several frameworks. For example, COBIT-4, NIST 800-53, and NIST 800-66 share a significant number of common controls.

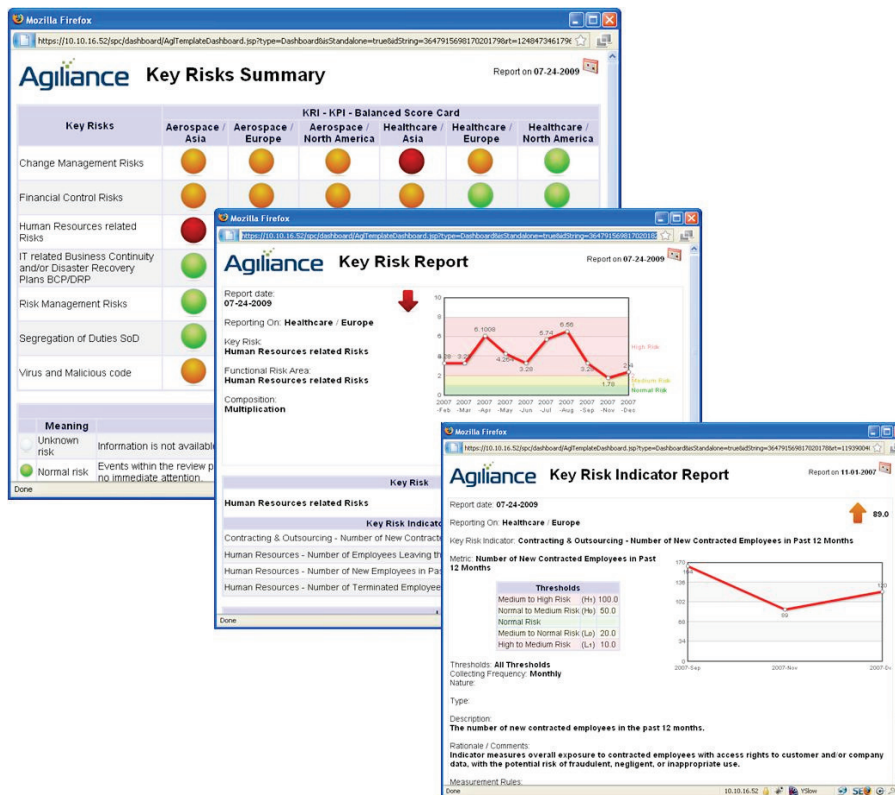
To further reduce cost and complexity and improve risk management effectiveness a key step is to employ a common control framework. By using a common control framework, one assessment, rather than multiple, will suffice to certify against any number of regulations.

The common control framework creates a central repository that maps standards, regulations and corporate policies. With a single enterprise wide control framework, there are fewer controls to test and independent assessments are unnecessary. Cost is lower as more work is done faster with potentially fewer people. With Agilience, agencies can test once and certify against many regulations.

## Manage risk

Risk scores provide decision-makers with insight and visibility. Once the business knows which risks matter, the next step is to take action to manage those risks. Actions include:

- Transferring a risk to another entity
- Avoiding a risk
- Reducing the negative effect of a risk
- Accepting some or all of the consequences of a risk.



With Agilience RiskVision Enterprise Risk dashboard, , agencies can employ economic impact measures such as the Annual Loss Expectancy (ALE) to further optimize allocation of its resources on prioritized risks. For example, an Enterprise Risk Model could be based on the impact of NOT implementing versus implementing new mandates that are not currently funded or budgeted.

Taking action on risk typically involves change management: A configuration change, a procedural change, or the development and deployment of a new policy and/or new controls to name a few. These changes must be defined, planned, approved, communicated, executed and verified.

Over time, the organization will see the effectiveness of its preventive and corrective actions through periodic risk assessments and controls testing as well as through its business results.

Agilience supports trouble ticketing and/or integrates easily with an existing trouble ticket management system already in place and it ensures that the links between prioritized risk, actions and results can be tracked and completed.

## Track Enterprise Risk Trends

Key Risk Indicators, also known as KRI's, are a measure used to indicate how risky an activity is. KRI's are used to measure trends based on a set of metrics that collectively indicate an overall risk condition. KRI's are presented in executive-level dashboards enabling management to respond with policy or strategy changes. The Agilience RiskVision dashboards are an intuitive, simple, color-coded early warning mechanism (i.e. Green, Yellow, and Red) and allows for the normalization and comparison of risk regardless of initial metric ranges.

Agilience supports a flexibility model for setting risk thresholds based on the agency "risk appetite" and escalation steps will multiple layers of drill down to root cause metrics. The Agilience KRI architecture includes Functional Risk Area, Key Risks and Individual KRI's.

## Conclusion

Agilience GRC Solution enables Federal Agencies to provide a unified Risk and Compliance view to all executive level constituents in an organization, which minimizes overall agency program risk, assesses the security and compliance of IT technology and demonstrates continuous compliance based on real time survey and automated control detail.

The Agilience GRC Solution enables Federal Agencies to:

1. Establish proactive IT security and risk posture, using objective business metrics
2. Unify the business by basing decisions on objective risk metrics tied to strategic goals
3. Federate vendor and partner risk assessments, using easy, Web-based, delegated surveys
4. Manage entire process by using dashboards to monitor progress at every step
5. Prioritize IT investment based on risk value and compliance criticality
6. Automate manual surveys and leverage existing investments in security and network tools
7. Leverage risk and compliance management - Test once, comply to many regulations
8. Decreased time to compliance - the first time and every time thereafter
9. Increased audit efficiency and effectiveness by reducing FTE requirements by up to 70% and audit consulting budgets reduced by up to 80%
10. Reduced risk by dramatically reducing compliance and security incidents
11. Proactively manage IT security and risk posture
12. Extend liability to vendors and partners as appropriate
13. Better IT decisions by communicating dollar value of compliance and security programs
14. Prioritize IT investments based on risk.

## About Agilience

Agilience ([www.agilience.com](http://www.agilience.com)) is a leading provider of enterprise Governance, Risk and Compliance (GRC) solutions. Founded in 2005, the Agilience GRC solution enables organizations to manage their IT and operational risks more effectively, while reducing the cost of meeting compliance mandates. The Agilience RiskVision™ is a fully integrated suite of GRC solutions, delivered on a purpose-built GRC technology platform. Global Fortune 5000 companies leverage Agilience's award winning technologies to address ever more demanding GRC requirements and complex security threats. The Agilience RiskVision platform offers an agile, modular approach to deploying GRC so that customers can meet their specific GRC requirements. The RiskVision suite includes five key GRC applications: Policy Manager, Compliance Manager, Enterprise Risk Manager, Vendor Risk Manager, and Incident Manager. RiskVision has received the highest rating of "Strong Positive" in the latest Gartner MarketScope for IT-GRCM, as well as the highest rating of "Leader" in the latest Forrester Wave for IT Risk and Compliance Software.

For more information:

Agilience Inc  
2001 Gateway Place, Suite 315W  
San Jose, California, 95110  
Phone: (408) 200-0400  
[sales@agilience.com](mailto:sales@agilience.com)  
[www.agilience.com](http://www.agilience.com)