Agiliance®

BUDGET RELIEF STRATEGIES

7 Tips to Beat the IT Compliance Budget Crunch

Sara Gates, Vice-President of Strategy - Agiliance, Inc.

ABSTRACT

Caught between tough economic conditions, competitive pressures and escalating compliance requirements, CISOs and other risk and compliance professionals face a daunting dilemma. Successfully balancing today's risk management, cost reduction and compliance equation can be difficult – especially in these uncertain times. As security incidents and new regulations continue to grow in number and complexity, businesses often divert precious staff time and operating budget away from growth-supporting initiatives to reactive activities such as regulatory audits. With the crumbling of Wall Street, companies can expect compliance's complexity and cost burden to grow exponentially as the government responds to current risk management inadequacies with an onslaught of new rules and regulations.

As demands to control the bottom line increase and regulators become even more aggressive, over-investing in compliance-related programs can negatively impact a company's ability to fund future growth initiatives. For businesses that want to break out of the current inflated threat and compliance-driven spending model to develop a more resilient and cost-effective IT risk management process, this paper offers budget-saving tips, ideas and solid practices for keeping up with compliance demands and more effectively allocating IT budget and resources based on business objectives.

TABLE OF CONTENTS

Executive Summary

It is time for IT to have its own relief plan. Caught between tough economic conditions, competitive pressures, and mounting compliance demands, today's IT faces an epic dilemma.

To remain resilient in this environment, businesses must contain costs while continuing to drive innovation and optimize performance. This translates to IT doing more with limited—or sometimes declining—resources.

According to a new survey by Forrester Research, Inc.[1] of nearly 950 senior IT managers across North America and Europe, more than 40 percent of large businesses have cut their IT budgets this year due to the global economic slowdown.

Due to the current global economic crisis, new regulations will continue to grow in number and complexity. Currently, there are more than 1,000 regulations in the U.S. alone, and Gartner predicts that by 2012, the number of regulations directly affecting IT will double. As security incidents and new regulations continue to grow in number and complexity, businesses often divert precious staff time and operating budget away from growth-supporting initiatives to reactive activities such as regulatory audits.

As a result, an increasing share of budget is being spent on IT security. Industry experts predict that the percentage of IT operating budgets devoted to security will increase in 2009 – despite tough economic times.

With this increased spending, many business leaders believe their current levels of investment in security and compliance may be out of balance. In the present threat-driven business climate, over-investing in compliance-related initiatives has the potential to hamper a company's ability to invest elsewhere, such as delivering new products and services.

As pressures mount to control the bottom line and regulators become even more aggressive, IT success requires the right balance of belt tightening paired with strategic investments required to fuel growth.

[1]Forrester Research, Inc. "The State Of Enterprise IT Services: 2008", September 2008.

How to Beat the Budget Crunch

Streamlining risk and compliance efforts can offer IT one of the greatest sources of budget relief. The new IT risk and compliance automation software solutions (sometimes called IT GRC) allow organizations to effectively manage risk and compliance for information-technology assets, people, and processes. These solutions provide the means to consolidate and integrate the plethora of technical data and to systematically gather, classify and prioritize security-risk data across assets, operations and regulations, thereby improving risk mitigation and reducing costs by automating manual, error-prone processes.

To companies in need of relief from exorbitant IT compliance-related costs, we offer the following 7 tips based on Agiliance's IT compliance automation and risk management expertise and knowledge of industry best practices:

Budget Relief Tip 1

Perform an inventory of IT and security infrastructure assets. Companies with multiple business units and subsidiaries often end up with geographically dispersed data centers and computing assets – making data collection and classification as required by regulations a time-consuming challenge. New technologies can connect to scanners, SIM/SEM, directories, CMDBs, identity management systems and other network products to help companies efficiently aggregate and reconcile data across diverse systems. Intelligent risk profiling can help IT automatically classify discovered assets and alert staff to inconsistencies or issues before auditors discover them. This frees up time spent on manual checking today and allows companies to focus on applying controls only to the most critical assets, leading to cost savings.

Budget Relief Tip 2

Automate collection of "tribal knowledge." Often, the best way to test a policy or control is to ask people in an organization and collect their responses. Collecting, analyzing, and reporting data can be slow, complex, and error-prone when relying upon paper-based surveys and manual data collection. Efficiencies can be gained by automating this collection process using auditable, automated, web-based surveys that gather data (from department managers, process owners, and system owners) and easily test responses against controls. Moving away from manual processes drives faster decision-making, more timely and cost-effective compliance, and provides the data for improved visibility across organizational boundaries.

Budget Relief Tip 3

Use technology to map compliance controls. Regulations are not specific regarding the exact IT controls necessary to satisfy compliance. As a result, one of the most difficult and time-consuming challenges for organizations is translating general statements of laws and regulations into specific and defensible controls for compliance. Manually mapping controls across regulations, standards and frameworks can be a full-time job. This activity delivers little business value to the company beyond keeping it out of trouble with regulators. Today's compliance solutions have already done the mapping. This allows companies to select the regulations, policies and standards that matter to them with a mouse click. Control testing becomes automatic – enabling valuable resources to return to more strategic responsibilities.

Budget Relief Tip 4

Streamline control testing and remediation efforts. Regulatory compliance depends on continuously monitoring and enforcing thousands of IT controls. Many organizations have problems detecting and addressing control violations in a timely manner. IT Risk Management and Compliance automation technologies can help alleviate these issues by automating testing, correlating and communicating control results to the owner(s) of the business risks. Integration with trouble ticketing and CMDBs can help expedite the remediation of control violations following formal change management methodologies. This also allows remediation efforts to be tracked from a single project dashboard.

Budget Relief Tip 5

Eliminate the process overlap. Large organizations typically must comply with multiple regulations, each with independent processes, metrics, and audit procedures. There is a 50-70% overlap between regulations in the questions they pose to organizations. With the imposition of each new regulation, the common approach has been to add a new compliance team with a new mission and scope. The final result? Multiple teams ask the same questions, creating significant inefficiencies and process overlap. In this situation, redundant processes, policies and controls are common – and teams interpret the same risk data differently. Compliance automation tools can help eliminate those redundancies, improve the consistency and quality of risk data, save time and reduce the demands on

managers by allowing companies to "test once, comply to many."

Budget Relief Tip 6

Focus on the most critical issues first. When companies depend on vulnerability logs and dashboard reports from multiple disparate security systems, it can be difficult to prioritize the criticality of control violations across a broad range of assets (processes, people and technology). The reliance on subjective opinions can make it difficult for business managers and executives to determine which issues are most critical and deserve scarce IT budget and resources – as a result, businesses often overspend on compliance. Having a single analytic solution that correlates data about processes, people and IT assets across regulations, frameworks, and controls can provide the intelligence needed to prioritize criticality confidently. This lets businesses focus on the most critical issues first and avoid unnecessary spending.

Budget Relief Tip 7

Develop a sustainable, continuous risk management and compliance infrastructure. Without a current and accurate view of IT risk and compliance status, companies expose themselves to greater risks of costly security breaches and audit failure. A persistent approach to IT risk management that tightly integrates the management of IT systems' security, compliance and risk can help companies avoid costly mistakes. A continuous compliance infrastructure creates a single system of record and a single source of truth for everyone involved in risk management – so everyone has the same consistent information. And it is always on so that everyone has a current view of the company's IT risk profile.

By tying together the interdependent disciplines of IT risk and compliance, companies can establish more accountable and effective IT security and compliance functions—without the high costs and inefficiencies of disparate programs.

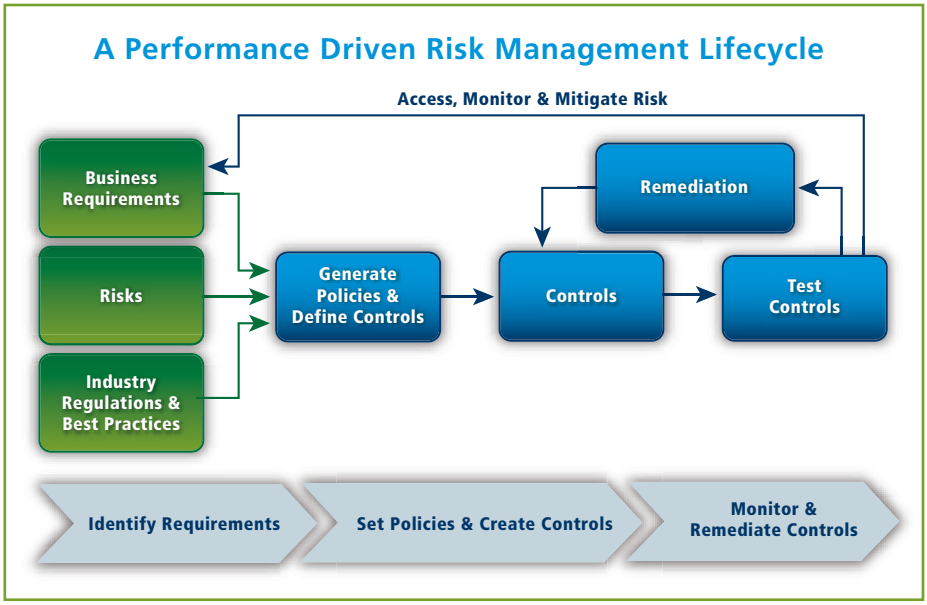
The Secret to Thriving in Chaos

Be proactive. Act Intelligently. The current U.S. financial crisis exists because of a failure in risk management. While Wall Street's crumbling is in the hot seat now, no industry is immune. Risk management can be poorly executed in all disciplines. Failures in risk management are also to blame for the personal information disclosure and malware crises. Crises emerge partly because executives don't understand their risks, and risk managers don't know how to talk to executives about risk.

Companies can expect the government to intervene and attempt to fix the current risk management failures with an onslaught of new rules and regulations—further adding to the complexity and cost burden of compliance without necessarily fixing the core risk issues. Companies have two choices: (1) continue to increase the proportion of IT budget spent on compliance as regulations grow, or (2) develop compliance and risk management processes to more effectively allocate IT resources and activities based on business objectives and acceptable levels of risk.

For businesses that are fed up with spending on security and compliance for its own sake, strategic investments in new IT risk management products can help companies evolve their risk management processes by providing current and accurate visibility into how IT risk affects the entire organization. With solutions that can normalize and combine risk from non-compliance with regulations and standards, IT security and system automation gaps and process-related risk can be consolidated into a dashboard view that provides business managers and executives the intelligence they need to make more informed decisions with confidence and ease.

In this manner, IT risk and compliance management solutions can support the growth side of the equation by helping



companies leverage existing security investments more effectively and by providing decision-makers with the current and accurate intelligence they need to understand better how IT risk affects their entire organization.

IT Policy Compliance Group[2], based on research conducted with more than 2,600 organizations around the world, found that companies with the most mature IT governance, risk and compliance practices performed, on average, 13% to 17% higher in customer satisfaction, customer retention, revenue, profit, and reduced expenses than those with the least mature practices.

In every down economy, there are opportunities to excel while others stand still. Companies transitioning from the current threat and compliance-driven business climate to a performance and risk-driven business process will be more resilient when new regulations are enacted and better positioned for success when the economy rebounds.

Forward-thinking companies can expect a realistic and well-executed IT risk and compliance program will pay dividends in lower costs, reduced risk, consistent compliance, and even better morale. With better security, lower audit burden, improved leverage of IT resources, faster decision-making and better optimization of existing business processes, companies will find themselves well-positioned to gain relief from the current budget crunch and build a strong foundation for future growth initiatives.

> *"Agiliance is leading the charge to provide companies in the medical field with the proactive and practical tools needed to ensure that security investments and compliance controls directly support their business objectives."*
>
> **– Kristen Knight**
> **Director**
> **Privacy Compliance at Philips**

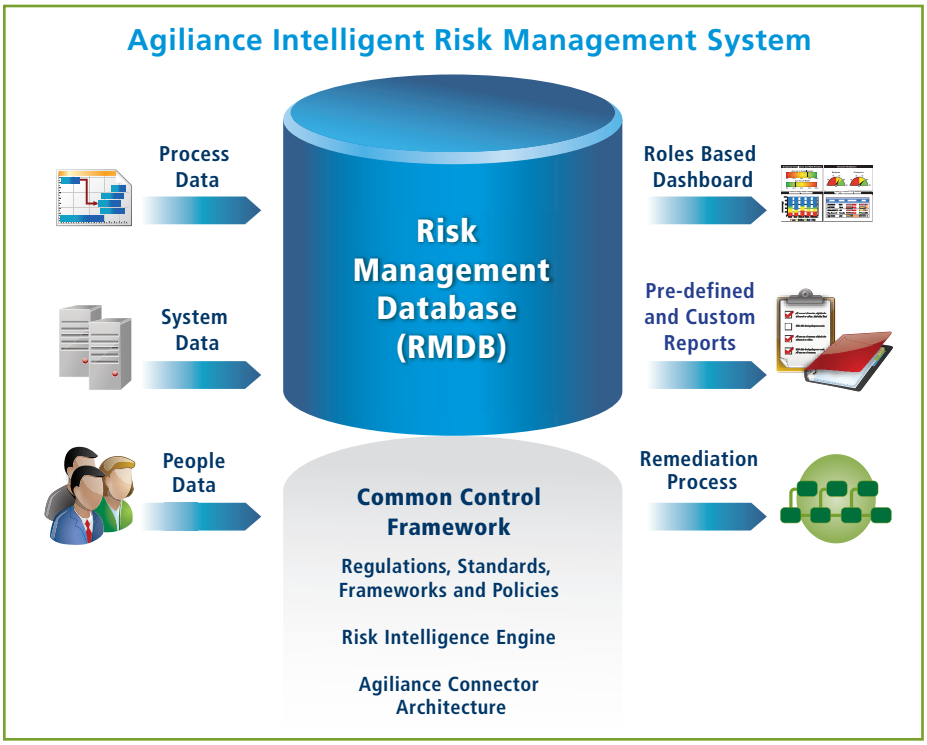
PHILIPS

[2]ITpolicycompliance.com, 2008 Annual Report on IT Governance, Risk, and Compliance: Improving business results and mitigating financial risk, May 2008.

Agiliance Risk and Compliance Solutions

Our customers, particularly in the government, insurance, retail, healthcare, financial services and energy sectors, face unprecedented challenges in managing IT budgets. They are being pressured to reduce expenses without jeopardizing compliance. By automating controls and compliance processes, enterprises can save millions of dollars in hard costs.

Agiliance offers highly automated IT risk and compliance management software to help organizations thrive under mounting pressures to manage and balance risk, compliance and IT budgets. By leveraging the power of Agiliance software, businesses can make impressive gains in their IT risk and compliance efforts, including reduced audit burden, increased visibility into current compliance and risk status, and improved leverage of IT resources.



"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

RSA

Agiliance Solution Benefits

To deliver customers the highest return on investment (ROI), Agiliance enables companies to aggregate and correlate risk data from systems, applications, people and processes into a single repository from which controls can be automatically assigned and monitored across the widest set of regulations and standards. In addition, we provide customers with the comprehensive IT risk management system they need to keep pace with the expanding requirements of IT compliance and operate at their highest level of performance. These capabilities allow enterprises to dramatically lower the cost of compliance and internal audits by as much as 70% to 80%.

MARKET NEEDS	AGILIANCE SOLUTION BENEFITS
Automate collection of people, process, and system control data	Agiliance software connects out-of-the-box with a wide range of IT and security infrastructure and enables extensive web-based self-assessments with the ability to import findings. In addition, automated workflow provides repeatable assessment processes. There is no need for custom development – Agiliance automatically aggregates and correlates data across systems, people and processes.
Automatically map controls from multiple regulations, standards and frameworks	Controls are pre-mapped across a wide range of regulations, standards and frameworks, including SOX, HIPAA, PCI, CobiT, ISO 17799, FFIEC, FISMA, NERC, GLBA, SB 1386 and more. With the ability to select multiple regulations, policies, security threats and frameworks with a click of a mouse, customer are ready to test controls in a matter of minutes instead of days or weeks as required with manual mapping exercises. And as regulations inevitably evolve or new assets get added, the Agiliance solution automatically updates controls to reflect the changes.

Test controls and eliminate process redundancies	Agiliance's hallmark "test-once, comply-many" capability eliminates duplicate testing across multiple regulations and speeds up the time to compliance. Using Agiliance's built-in Common Control Framework – containing over 10,000 controls across authoritative sources such as ISO 17799, ISO 27001/27002, NIST SP800, SOX, HIPAA, GLBA, FFIEC, PCI and many more – companies can test controls across all applicable regulations. Where redundancies exist, customers can test the common control one time to satisfy the requirements of multiple regulations. This eliminates the time and cost associated with duplicate tests.
Remediation and exception management	Agiliance automatically prioritizes IT assets such as servers, applications and network devices that need to be monitored for risk so that the most critical assets can be addressed first, e.g., those containing personal identification information, medical records or credit card information. Managers can immediately view the cost of downtime, the impact of various risk mitigation plans, the cost of replacing the asset and make real-time decisions about remediation versus accepting or transferring the risk. Automated ticketing insures mitigation processes are handled. Using this intelligence, decision makers can be confident that budget is being wisely allocated towards the most critical assets eliminating overspending on shotgun approaches that may add unwarranted controls across the entire IT environment.
Complete visibility into current compliance & risk status	Agiliance software provides decision makers with the current and accurate risk intelligence they need to better understand how IT risk affects their entire organization. Role-based dashboards and pre-configured report templates provide tailored views. Reports can be delivered to executives, managers or security analysts, with details by division, regulation, business process, or a host of other customizable views. Companies can rely on Agiliance to deliver continuous monitoring of risk and compliance across the enterprise – in the way that makes sense to them.

Why Agiliance?

As the costs and complexity of IT risk and compliance continue to rise, Agiliance believes that customers need practical solutions that are highly configurable, easy to integrate, and interoperate with the widest range of popular security and IT infrastructure systems. Our unsurpassed expertise in the interdependent disciplines of IT security, compliance, and risk, combined with our security automation and enterprise software acumen, allows us to deliver customers' integrated capabilities to mitigate risks and execute forward-thinking plans easily and confidently.

Agiliance is the only solution in the market with a unified Risk Management Database (RMDB) containing regulations, best practice frameworks, IT and standards. The solution maintains risk and compliance scores over time—serving as a single system of record for the approval and maintenance of corporate policies. In addition, Agiliance allows customers to incorporate external global feeds containing threat and vulnerability information to deliver the most comprehensive view of risk across the enterprise. Including information from human e-Survey processes, the system delivers an enterprise-wide view of risk.

"We're working with Agiliance because their product met our key criteria which include easy integration with our company's existing applications."

– Oliver Eckel
Head of Corporate Security
bwin Interactive Entertainment AG

bwin

ABOUT AGILIANCE

Agiliance offers highly automated IT risk and compliance management software products designed to help organizations thrive under mounting pressures to manage and balance risk, compliance, and IT budgets. Fortune 1000 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 understand better how IT risk affects their entire organization. Agiliance is headquartered in San Jose, California and is backed by Walden International, Intel Capital, SVIC, Red Rock Ventures and Castile Ventures. For more information, please visit www.agiliance.com.

Agiliance, Inc.
1732 North First Street
Suite 200
San Jose, CA 95112
p: 408.200.0400
f: 408.200.0401
www.agiliance.com