



Business Risk Intelligence

Bringing business focus to information risk

It's a challenge maintaining a strong security and risk posture.

CISOs need to constantly assess new threats that are complex and unpredictable. They must prioritize and remediate gaps in the security architecture, address evolving regulations and manage the audit process. And they must do it all without disrupting critical business processes. But above all that... The real challenge is to achieve true alignment:

... between business strategies and risk management

... between operational priorities and security investments

... and between market performance and regulatory compliance

That's what Allgress Business Risk Intelligence ensures.

By offering instant, accessible and visual analysis of the risk impact of each corporate initiative, Allgress elevates the role of the CISO to focus on minimizing risk, creating company-wide value, and supporting business objectives.

- Allgress empowers security organizations to paint a transparent picture of their holistic risk posture that is consistent, repeatable and defensible.
- Allgress helps security organizations demonstrate in concise and concrete terms the management justification for specific plans, projects and expenditures.
- Allgress facilitates the defense of budget requirements and expenditures; shows why they are necessary; and how they will effectively manage risk and enable the business.

That's Allgress Business Risk Intelligence. That's GRC re-imagined.

Business Risk Intelligence provides consistent, repeatable and defensible metrics to ensure that the right budget is being allocated to the right areas at the right time.

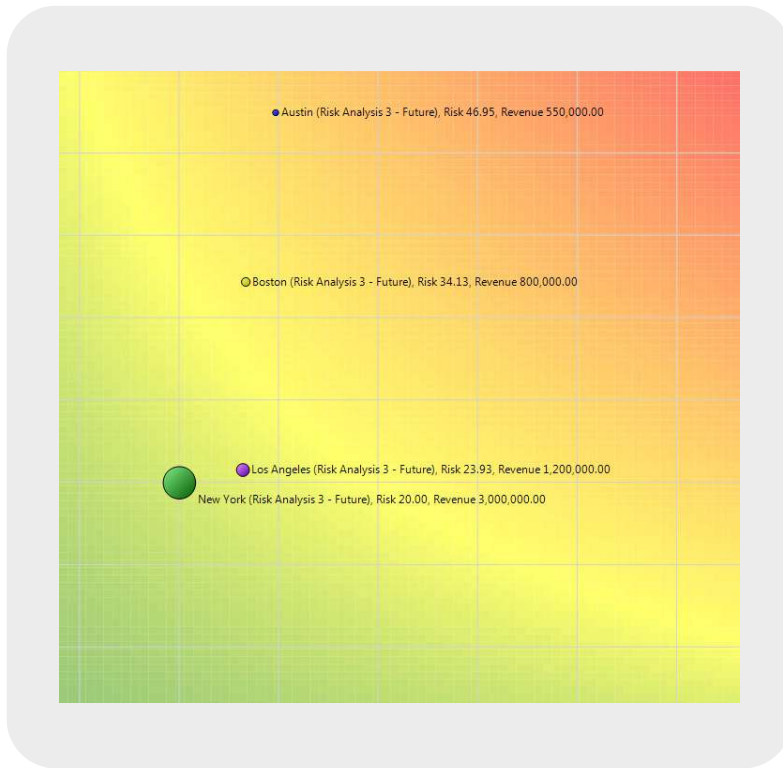
Even with sophisticated Enterprise Risk Management (ERM) and Governance, Risk Management and Compliance (GRC) programs in place, the process is mostly manual. Working with thousands of spreadsheets and other data types is a significant effort that makes it cumbersome to compile risk reports that show where the business is, how it's trending, and where the gaps are. At best, risk reports are inconsistent and incomplete, lacking all the inputs and variables. At worst, they're inaccurate, outdated and misleading, lacking any context. Most of all, they don't take a higher business view.

Allgress GRC re-imagined takes these processes to the next level: business risk intelligence tools help CISOs dealing with a fast-moving business environment to break free of the usual constraints. Streamlined workflows, ease of implementation, and superior reporting and analytics help verify and support your security programs and initiatives and demonstrate in real time the true impact of changes on the security posture.



Allgress Business Risk Intelligence

Allgress Business Risk Intelligence helps companies quickly and automatically aggregate massive amounts of data—from security and compliance assessments, vulnerability scans, ERM, GRC, DLP and web applications and many other sources—and turn it into meaningful, actionable risk-specific intelligence.



Risk and associated business impact helps security executives make decisions quickly.

Allgress BRI builds on an innovative blend of software, services and automated processes to offer consistent, repeatable, and defensible analyses that paint a visual and comprehensible picture of holistic risk. Effortless dashboards build on historical patterns, current and trending data, and evolving compliance mandates, to assess true business risk as it affects top-line business performance issues and bottom-line costs.

With our flexible, easy to use tools, you can identify risk areas that are under-exposed and reorder security priorities to better align with the current business environment. Trending techniques, business modeling and what-if analyses offer a clear balance between past, present and pending threats to the business.

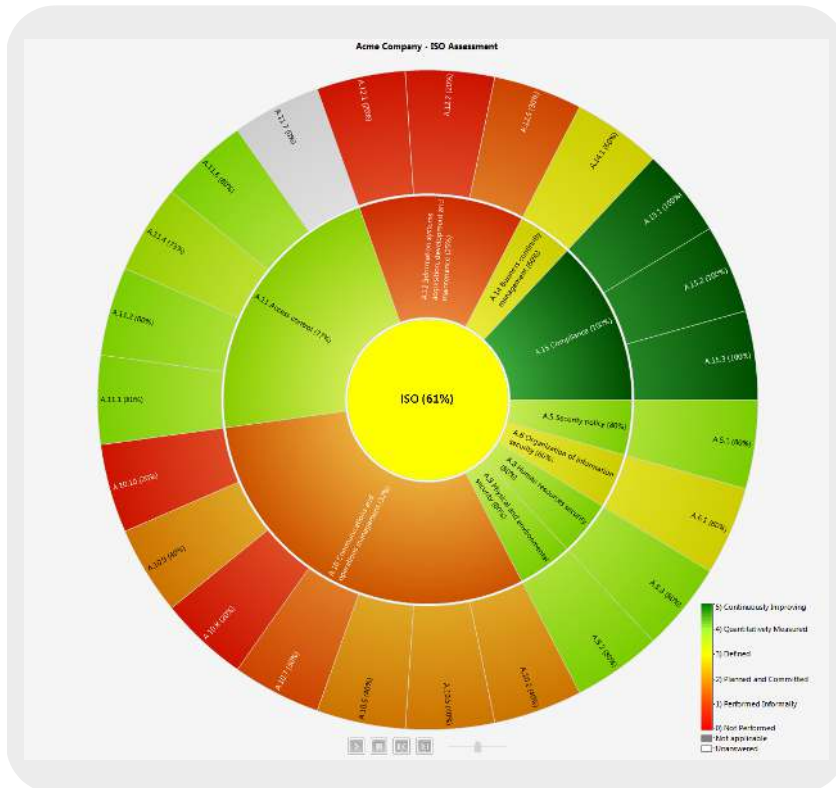
Business metrics map to key performance indicators, clearly showing how specific management initiatives such as budget directives, product innovation, security implementations, and other issues change the risk picture and affect business results. You can clearly outline the road ahead with a focus on short- and long-term benefits, risk and loss reductions, regulatory changes, process improvements, and more.

Allgress provides:

- **ease of use.** No more complicated pivot tables or macros necessary.
- **flexibility and adaptability.** A model that can adapt to your specific performance indicators to create a holistic picture of risk.
- **risk exposure over time.** Show your risk reduction over a period of time—or explain why risk has increased as a result of the reduction of information security resources.
- **what-if scenario creation.** Align information security strategy with business objectives. Is there a new initiative to enter new markets? Is security prepared to protect those investments and new customers? Are new mergers and acquisitions increasing risk? What resources does security need to manage risk—and where should those resources be deployed?
- **consistent, repeatable, defensible metrics.** Based on widely-accepted standards, your methods are easy to repeat and show to critical stakeholders through out the organization.

Allgress Security and Compliance Assessment

Allgress Security and Compliance Assessment helps companies simplify the audit process. A clear, straightforward workflow process leverages common requirements to minimize tasks while generating reports that easily meet a range of compliance needs.



Easy-to-interpret graphs are a click away. View detailed information by drilling through the data.

Your environment changes constantly: resources come and go, and risk analysis methodologies get evermore complex. That makes it difficult to determine information security risk. But while security assessments shouldn't need to be driven by compliance mandates, many know it's not a choice: Regulatory agencies and requirements state that companies must maintain a risk program and regularly perform risk assessments.

Added to that, regulatory compliance is not a one-source problem: Companies must deal with multiple government agencies and regulatory mandates, industry requirements and standards, with shifting changes and evolving deadlines. The process is complex, time-consuming, and costly.

Allgress Security and Compliance Assessment solves these issues.

Allgress provides:

- **standard-to-standard mapping.** Take one assessment and see how it measures against other standards, cutting the time required to complete assessments and reusing data from one assessment for other audits.
- **operational efficiency.** No more spreadsheets, just automated and continuous assessments.
- **flexibility.** Manage third-party business partners and create your own surveys and custom standards to ensure adherence with your information security program and requirements.
- **efficiency.** Many companies already have internal and external audits and security assessments, and Allgress leverages those efforts to generate rapid risk assessments.
- **reporting and analysis.** Assessment reports can be generated and customized based on organizational business units, OS platform, or any other category that suits the business.
- **workflow management.** Track ISO, PCI, HIPAA, SOX, and other compliance activities with a user-centric workflow.
- **standardized installations.** Specific solutions for your industry—financial, health care, energy, and more—are available to get you working even faster.

Allgress Vulnerability Management

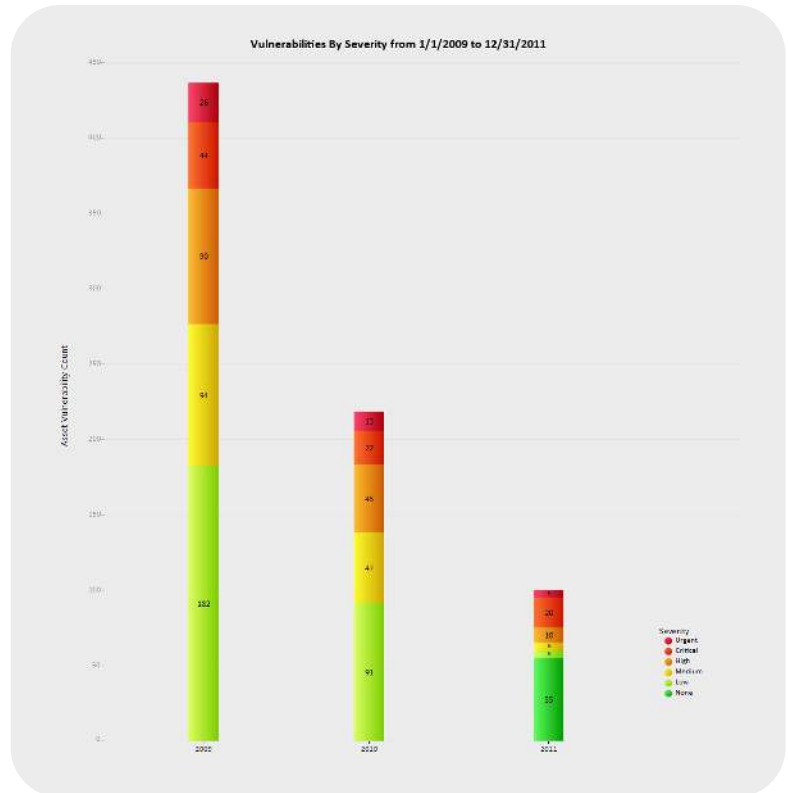
The scanning technology is in place, and every key system is continuously monitored. But under the mountains of data, trends are emerging that could detail future risk. Can you see it? Can others see what you see?

The Allgress Vulnerability Management Module provides a complete solution to help analyze and interpret the vast quantities of vulnerability data in a transparent and consistent format that helps drive strategic business decisions.

Best-in-class graphics, combined with the powerful Allgress Reporting Engine, provide instant insight into key metrics for mission-critical systems. Allgress supports a constantly evolving variety of source data (including network, application and wireless) to provide flexibility for your technology choices.

With this patented solution, you can sort and filter data the way you want to see it. Allgress cuts through layers of vulnerability scanning to summarize important tasks and divide the work among business units. Import multiple scan sources and instantly see a snapshot of the threats that need to be mitigated immediately. Move away from using spreadsheets as a reporting engine.

Allgress Vulnerability Management integrates with your existing infrastructure, and enables full-scale rapid deployment in weeks-not months. Manage all aspects of your vulnerability management from a single location with a few simple mouse clicks. No extra burden on IT staff, no additional investments in software-just faster time to value.



Trending and time-series views make it easy to see the count and severity of your vulnerability data.

Allgress provides:

- **a centralized data store.** Consolidation and filtering of all scanning data (vulnerability, DLP and other sources) is available from a single store. You can compare business units and network segments to see where threats are most prevalent so that you can prioritize resource allocation.
- **mitigation and management.** Remediate all of your issues in a single project—no matter where they originated.
- **false positive management.** Find all known false positives or vulnerabilities that have compensating controls, then filter them so that you can prioritize the real security threats.
- **an agnostic view toward scanning.** Allgress supports all major scan vendors so that you're not locked into a single solution. Allgress normalizes the inputs from multiple scanners to provide a consistent level of criticality.
- **time-series comparisons for scans.** View real-time progress toward mitigation of your critical issues.

Allgress Incident Management

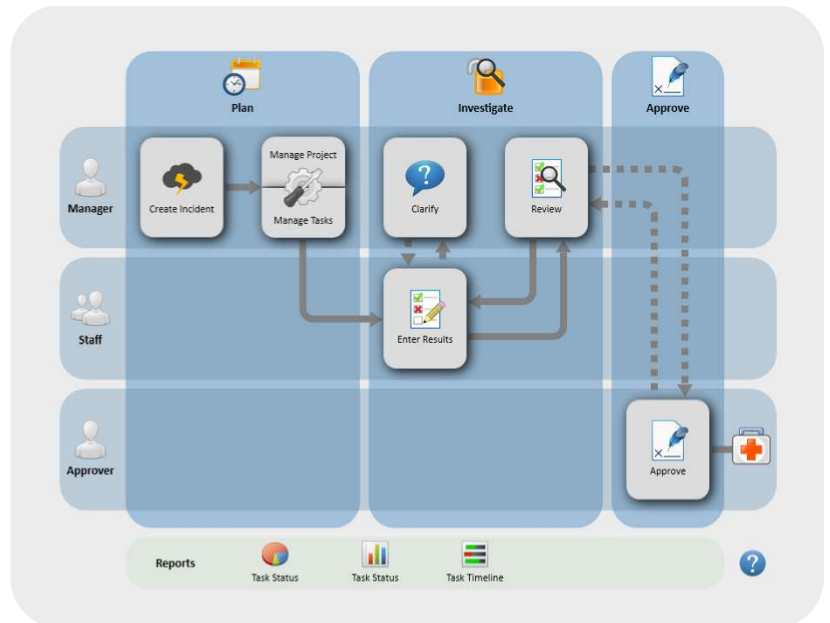
Today's operational environment encompasses a staggering array of security threats, from the physical theft of backup tapes to coordinated botnet assaults that play out over months and are conducted by teams of sophisticated hackers around the world. That's why it's virtually impossible to define a set of requirements that covers every possibility in every investigation.

By building on the right experience with the appropriate skill sets, it is both possible and helpful to have a centralized document collection site with built-in information gathering templates that allow for consistent collection of evidence and investigation data in the aftermath of an incident. Security staffs operate from a single repository, creating a unified approach to incident reporting, collection, and investigation. By prioritizing responses, tracking incidents to their completion, and providing a way to ensure that future practices prevent deficiencies, teams can effectively mitigate incidents.

In capturing every incident, Allgress Incident Management helps generate reports that show the type and severity of issues and the organizational response, giving executives the ability to maintain situational awareness in order to anticipate necessary actions, and the ability to make sound and timely decisions.

Allgress provides:

- **focused response.** A centralized repository collects evidence and investigation data to handle incidents and intrusions.
- **an all-in-one solution.** Dedicated components for incident triage, incident coordination, and incident resolution provide a place to build a consistent methodology.
- **prioritization.** Manage incidents based on their overall business impact.



Simplified workflows make creation of incidents and investigation more streamlined and efficient. These workflows are available throughout the product.

Allgress, Inc.

111 Lindbergh Avenue, Suite F
Livermore, CA 94551
925.579.0002
www.allgress.com

