White paper

CAST
ACHIEVE INSIGHT. DELIVER EXCELLENCE.

structural quality
an Atos quality approach for the digital age

Your business technologists. **Powering progress**

Atos

Introduction

The current wave of transformation towards truly digital enterprise models affects all organizations worldwide. As a result, the application landscapes that IT Systems Integrators deliver, maintain and transform are growing exponentially. Applications are becoming increasingly critical in companies' core business processes, in client interactions, in decision mechanisms, productivity and time-to-market. As a result, the current revolution in IT for enterprises is digital business transformation across the entire value chain.

In the wake of this revolution systems integrators continuously adapt, amend and improve delivery methodologies and tools, allowing them to keep ahead of the pace of change required by their customers.

While IT leaders strive to meet increasingly complex functional requirements within shortened timelines, it is more important than ever to measure and manage the non-functional health and 'structural quality' of enterprise applications. Without doubt, structural quality is the foundation of the holistic health of applications and significantly affects their operational quality and Total Cost of Ownership (TCO). De facto industry standards specifying the quality of applications focus on dimensions of reliability, performance efficiency, security, scalability, usability, latency and maintainability.

In this white paper, Atos analyzes how an industry leading solution for application code quality and functional size measurement such as CAST impacts application health and quality aspects. We illustrate how a Tier-1 systems integrator can leverage such a tool to deliver the premium quality mandatory for the global digital revolution organizations are going through.

Contents

Introduction 2

The impact of structural quality 3

- Structural quality – an industry standard
- Assessing business risk through software quality
- Complexity drives Total Cost of Ownership

How CAST helps to detect issues and how to derive measures for improvement 4

How Atos applies cast in service transition 5

How Atos applies CAST in application maintenance 6

- Spanish Regional Government

Driving improvements in application reliability and performance 7

- Automated function point counting: the basis for productivity measurement

How Atos uses CAST to improve application security 8

- Why is Secure Coding key for future-proof applications?
- Atos Secure Coding policy
- Education and awareness
- Source Code analysis
- Fixing security violations 9
- Architectural security

Innovation with CAST 10

- Application portfolio analysis, powered by cast
- Application cloud-readiness assessments
- Proven enterprise architecture practices to support the migration
- Driving innovation in software development

Conclusion 11

The impact of structural quality

...or the lack thereof

Structural quality – an industry standard

Structural quality describes the extent to which an application's architecture and source code avoids well-known software flaws and is consistent with software engineering principles and best practices. It mostly drives non-functional quality attributes, such as reliability (uptime), performance and security.

The Consortium of IT Software Quality (CISQ) prescribes four software quality characteristics in their Software Quality Specification: reliability, performance efficiency, security and maintainability. CISQ was formed by the Software Engineering Institute (SEI) at Carnegie Mellon University, and the Object Management Group (OMG) to develop standards for automating these measures.

Structural quality can be measured at the code level and at the application level. Most applications are made up of many components, typically using different languages such as Java, C# and PL / SQL. These components are typically separated into tiers, such as the front end, app server, SOA services, some legacy components, and database. Code quality at the component level can detect some simple best practices and ensure the code is readable. In contrast, structural quality at the application level will address more serious flaws that may have an impact on the customer or the business user.

Assessing business risk through software quality

The structural quality of an application portfolio is a strong indicator of the risk within enterprise software and its impact to the business. Strong empirical evidence correlates structural defects to post-production flaws. According to OMG, "Bad software engineering practices at the Technology and System Levels account for only 8% of total defects, but consume over half the effort spent on fixing problems, and eventually lead to 90% of the serious issues in production." [1]

Poor application-level structural quality causes many high-impact business disruptions such as application outages, security breaches, corrupted data, and performance degradation. Industry data also demonstrates that poor structural quality creates enormous waste in the form of rework – 30% to 50% of application development effort in most organizations comprises rework.

Complexity drives Total Cost of Ownership

A significant component of an application's total structural quality is its complexity. Application complexity impacts the TCO of the software, since complexity increases the efforts needed to maintain and enhance the application. In this context, the drivers of effort can be described as (a) how easy it is to change the code without negative impacts, and (b) how easy it is to transfer the application from team to team, developer to developer.

Properly designing a new application and managing the complexity of an existing application can often have profound impact on its TCO. The same concept can be applied at the portfolio level. By understanding and evaluating the overall complexity of the portfolio, IT leaders can thoughtfully manage their spend on application maintenance and development. Gartner states that only 8% of an application's TCO that will be in production for 10 – 15 years are spent on design and implementation, yet it is in this phase where 92% of the cost can be influenced.[2]

[1] Object Management Group, "How to Deliver Resilient, Secure, Efficient, and Easily Changed IT Systems in Line with CISQ Recommendations", http://www.omg.org/CISQ_compliant_IT Systemsv.4-3.pdf

[2] Gartner, "A Framework for the Lifetime Total Cost of Ownership of an Application"

How CAST helps to detect issues and how to derive measures for improvement

Increasingly, within the IT community, there is a growing acknowledgement of the benefits of moving quality initiatives earlier in the lifecycle. The figure below describes the relative cost of a defect as the defect moves from requirements to production.

Traditional testing focuses on Functional Testing and Performance Testing of deployed code. These are performed at the tail-end of the Software Development Lifecycle (SDLC) which inevitably leads to late discovery of defects. Traditionally, testing for security vulnerabilities are also performed very late in the SDLC and QA process. Critical functional defects and major performance issues discovered late in the SDLC causes delays in deployment to production. Many of them may even call for architectural and design changes resulting in business disruption and increased costs. The industry is moving quickly to a model where defects are unearthed early by adopting **Shift Left** techniques.

The use of CAST for static code analysis is a key component of application delivery and quality control at Atos. From a quality standpoint, running a CAST assessment as a tollgate helps the testing team understand the following via Structural Quality Factors:

- **Robustness** – has a direct correlation to the level of regression testing for a release / change
- **Security** – gives insight into the application's vulnerabilities prior to dynamic security scans and testing
- **Performance** – this identifies potential bottlenecks prior to the performance testing of the application
- **Changeability** – the ease of application change indicates the level of testing required to ensure quality.

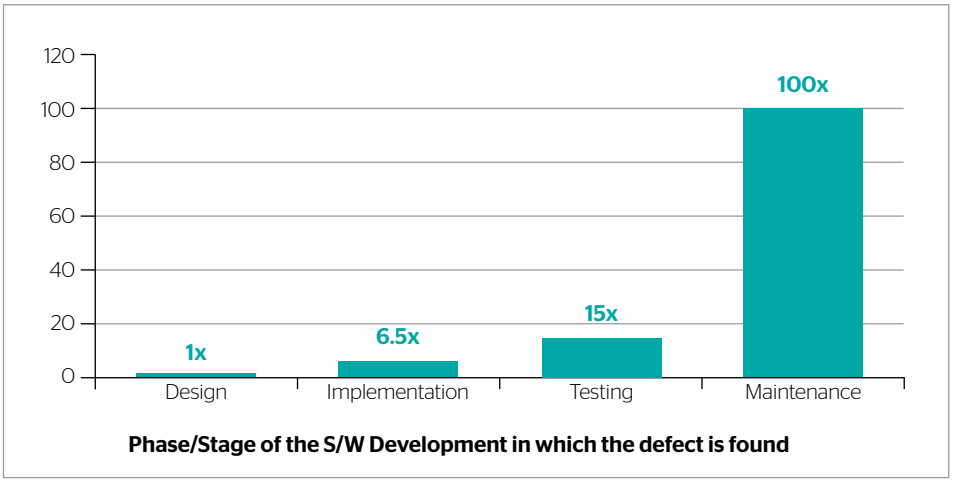


Figure 1 – Relative Costs to Fix Software Defects (Source: IBM Systems Sciences Institute)

Shift Left is the practice of focusing on quality from day one of a project in order to identify and fix defects as they arise. This reduces the increased costs and effort associated with fixing defects at later stages of a project when timing is most crucial.

Success story

Transport organization

- Accelerated newcomer onboarding
  - Effort saved for creation of technical documentation using CAST on CrewPlan **25%**
  - Effort saved of knowledge transfer during transition due to CAST documentation **19%**
  - Enhanced feature request / impact analysis processes
  - Effort saved for complex tickets during impact analysis with CAST **21%**
- Resource rationalization
  - Factory model allows for resource efficiencies. **6.8%**

How Atos applies CAST in service transition

Atos uses CAST both during development to intrinsically build-in structural quality and also during service transition to operations. We use CAST in service transition in order to baseline the quality of the delivered solution and thus ensure that the ongoing support maintains the delivered structural quality against the defined parameters.

CAST also helps project teams with faster knowledge transfer as well as faster onboarding for new team members by providing blueprints of the applications concerned. CAST generates the following specific technical documentation for applications:

- Entity relationship (ER) diagram
- High level architecture view
- Database access view
- Transaction / workflow view
- Application interfaces.

As most of the technical documentation for applications can be provided directly from the tool, project teams are able to put more focus on functional aspects during knowledge transfer. CAST thus enables a fast learning curve for maintenance and operations teams.

CAST is used to identify complex and risky modules in applications, so developers can spend more time and effort on those modules to gain a better understanding of application architecture. Project teams are further able to prioritize and schedule trainings based on the complexity of applications as defined by the CAST analysis and blueprint.

A CAST dashboard clearly shows the overall intrinsic weaknesses of a system or application within the portfolio. Using this analysis, Atos project teams can fully understand the most frequent quality issues and remedies. Similarly, CAST helps to identify 'dead code' in an application, so that developers can optimize and remove redundancy. The analysis also helps our developers to focus on:

- Applications with greater coding complexity and lower 'Transferability Indexes'
- Applications with overall low health factors scores
- Applications with high ratios for number of violations / lines of code.

All of this ensures that project teams easily gain knowledge of dependencies between different modules and technologies at source code level. Based on this knowledge of structural properties of applications, organizations are better able to select the right skills and team competencies to rigorously support the applications.

At Atos, we have used CAST for many application development, optimization and maintenance contracts, examples being Nokia, Acerta, RLA and BMW.

Success stories

Increased productivity and faster onboarding

Transport:

- **Ticketing Apps**
  Estimated effort saved for creation of technical documentation using CAST. **69%**

Healthcare:

- **Mainframe assessment**
  Effort saved during knowledge transfer due to CAST documentation. **50%**

Insurance:

- **Application documentation**
  Effort saved of KT during knowledge transition due to CAST documentation. **50%**

Success stories

Faster change implementation:

- **Microsoft landscape for an insurance company**
  Effort saved during Impact Analysis with CAST. **47%**
- **Mainframe landscape for an insurance company**
  Effort saved during Impact Analysis with CAST. **60%**

How Atos applies CAST in application maintenance

Currently, Atos is using CAST in application maintenance in five key areas:

1. **Portfolio risk management:** to have a global view of the quality, risk status and trends of applications
2. **Remediation:** to solve detected technical pains in applications
3. **Ongoing quality improvement:** to regularly measure the quality of applications using structural quality gates
4. **Impact analysis of change requests:** securing and improving accuracy and response time of change requests
5. **Actionable improvement plans:** CAST analysis provides the vital application quality and compliance visibility to the quality management team so that they may mitigate and plan carefully to avoid repeat defects and SLA failures.

Many project teams in Atos use CAST to enhance application maintainability, by reducing maintenance cost and time, and quality metrics, by resolving defects before they reach production, through goal oriented action plans. This results in far more predictable, stable application operations in the business.

We have two distinct approaches to deliver application quality improvement services using CAST:

1. **Corrective improvement program for customer satisfaction improvement and service improvements:**
   - Determine targets based on pain points, customer business and operational goals
   - Initial causes and weaknesses audit (scan) and analysis
   - Determine improvement actions (cost / benefit of each actions)
   - Campaign of improvement actions executions
   - Improvement control audit and remaining residual weaknesses audit
   - Corrective actions
   - Final code audit against initial targets

2. **Preventive, continuous improvement campaign to reduce the risk of future defects and service level impact:**
   - Determine targets
   - Initial scan
   - Set-up improvement actions to be executed during each patch or functional release
   - Regular scan to follow-up improvements as well as setting new targets.

Success story

Healthcare

- Accelerate induction phase of newcomer
  - Effort saved during knowledge transfer due to CAST documentation **50%**
  - Earlier Detection of Defects / low productivity practices
  - Time saved by team in proactive maintenance using CAST **33%**
- Quality Monitoring
  - Quality of application maintained (validation by CAST as Quality Gate) since baseline over last five releases building customer confidence.

CAST generates end-to-end cross-technology analysis maps with pre-identified dependencies between application components. This ready-made technical documentation shortens the learning curve and reduces resource attrition. Also, the resulting technical documentation can be used for impact analysis of change requests making request resolution faster and more effective.

In Atos, CAST is used during steady-state application maintenance projects for many contracts like Nokia, TDF, AIRBUS, Munich RE, FirstGroup, Benjamin Moore and FHLB.

Spanish Regional Government

The Cantabria Regional Government wished to see how it could make their project Yedra more interchangeable and whether new modules could be added on easily. They contacted Atos to help them with the necessary audit and documentation.

Using CAST we could visualize some of the main characteristics of the application to the project team. This was key to understanding all interdependencies.

This 11-year old legacy system not only had over two million lines of code with a lot of dead code, duplicated code and coding elements (Java Server Pages) that could not be compiled, it also completely lacked patterns or frameworks. No wonder the application was nearly unmanageable. Yet most interestingly of all, there was no documentation – a common weakness in legacy systems that can now be largely overcome with CAST.

Feedback from Celestino Güemes Seoane, Director of Innovation:

"Although the Yedra CAST Analysis has been just one part of the whole proposal, we think it has been a quite important one, because the client was very satisfied with the results. So I would like to thank your support, that has been very important for us during the analysis phase."

Driving improvements in application reliability and performance

What are reliability and performance efficiency industry best practices?

Reliability industry standards focus on areas such as: error and exception handling, data access through multiple layers of the architecture, inheritance and polymorphism.

Performance efficiency industry standards focus on areas such as: expensive calls in loops, memory and space management, SQL and data handling, and dynamic instantiation.

Applications that are unreliable impose significant financial risks on organizations that range from revenue loss to litigation. More importantly, poorly performing applications can cause severe user dissatisfaction and loss of business productivity.

Atos helps customers detect and address reliability and performance issues by using CAST. This deep software analysis and measurement technology enables Atos to focus on the most significant reliability and performance issues within our clients' applications. Hotspots identified by CAST are highly actionable due to its basis in application-level analysis, industry standards and proven correlation to post-production defects.

Atos typically provides reliability and performance enhancements using two approaches:

1. **Periodic assessment** – Atos analyzes the client's application code on a pre-determined frequency, which is commonly two to four times a year. Then, the highest priority issues are documented and addressed along with the next development or maintenance cycle
2. **SDLC integration** – integration of CAST into the SDLC process. This can range from a single pre-release analysis to stop critical issues before production, to in-process scans at key milestones of the development cycle which enables continuous improvement throughout the process.

Both approaches result in measurable reliability and performance improvements.

Automated function point counting: the basis for productivity measurement

Atos strives to develop and maintain applications with the highest possible quality. While application development and maintenance productivity used to be a mere black-box to many technology service providers, CAST's automated function point counting capabilities are starting to shed light on scale, measure and improve intrinsic quality for application portfolios.

One of the goals of measuring productivity at Atos is to continuously improve efficiency of the delivery centers. Functional sizing of applications, using function points (a standardized way to measure quantity of business functionality in software), is the foundation of application development productivity measurement.

With the introduction of CAST's automated function point counting capabilities, we are able to scale our productivity measurement program to very large applications and across a very high number of them.

More importantly, automating function points allows productivity to be consistently measured, removing the subjectivity of traditional counting.

With CAST's methodology firmly rooted in automated function point counting guidelines issued by the Object Management Group, Atos is confidently implementing a multi-center productivity measurement program to ensure that we are delivering the best possible service to our clients.

How Atos uses CAST to improve application security

Why is Secure Coding key for future-proof applications?

Web applications are the number 1 target of hackers

- 75% of attacks at Application layer (Gartner)
- XSS and SQL Injection are #1 and #2 reported vulnerabilities (Mitre).

Most sites are vulnerable:

- 90% of sites are vulnerable to application attacks (Watchfire)
- 78% percent of easily exploitable vulnerabilities affected Web applications (Symantec).

Web applications are high value targets for hackers:

- Customer data, credit cards, ID theft, fraud, site defacement, etc.

Atos customers ask for compliance with secure coding standards and best practices:

- Payment Card Industry (PCI) Standard
- Open Web Application Security Project (OWASP)
- Common Weakness Enumeration (CWE).

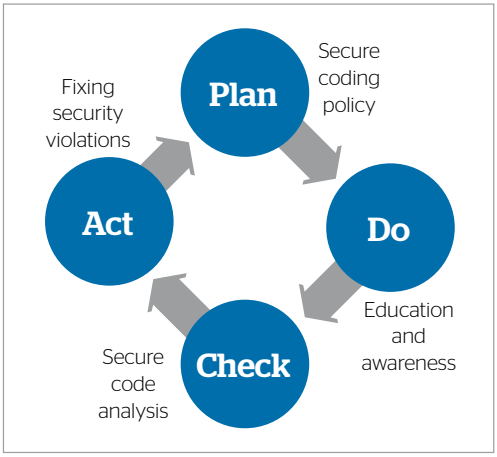


Figure 2 – Plan-Do-Check-Act (PDCA) approach for developing Secure Software

Atos Secure Coding Policy

The Atos Secure Coding Policy helps clients minimize the risks applications that were not designed or maintained with security in mind. This set of rules and principles is imperative for any application that connects to the internet or processes personal data. Our Secure Coding Policy includes requirements for critical topics such as input validation, session handling, access control and data protection.

Education and awareness

Our software development teams regularly receive appropriate training to stay ahead of the latest trends and to remain informed about Atos security policies. We often use CAST as a tool in our training programs for developers, since it gives practical insights about avoiding common pitfalls and best practices to adopt across the development lifecycle.

Awareness and training not only help ensure the creation of software with security and privacy in mind, it also guarantees that our development teams stay up to date on security issues.

Source Code Analysis

Source Code Analysis is the process of checking application source code for security issues. Many serious security vulnerabilities cannot be detected through any other form of analysis or testing such as Penetration Testing. These issues often manifest themselves as the most harmful vulnerabilities e.g. in web sites and thus Atos applies Source Code Analysis as a preventive measure in the development process.

CAST supports many areas of industry-leading research and standards on security vulnerabilities:

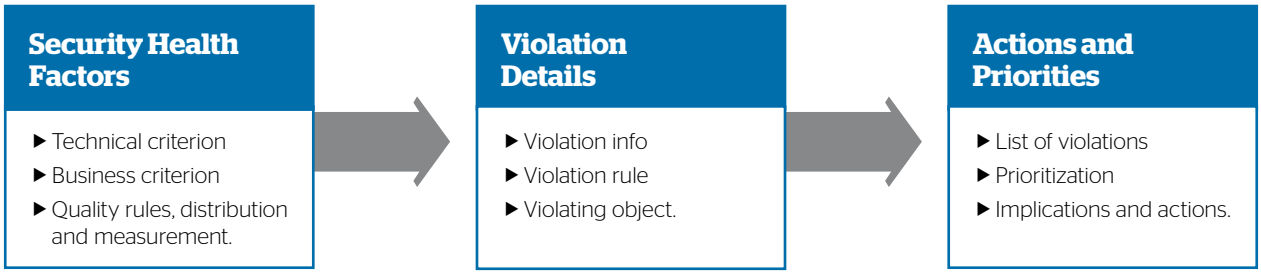
- The Open Web Application Security Project (OWASP) Top 10 -2013
- Common Weakness Enumeration (CWE) Top 25
- Payment Card Industry (PCI) Standards.

CAST Security

The Security Health Factor measures the likelihood of potential security breaches linked to coding practices and application source code and provides framework based rules grouped into three areas: Business, Technical and Quality, Distributions and Measures criteria.

Fixing security violations

From Secure Code Analysis to fixing security violations

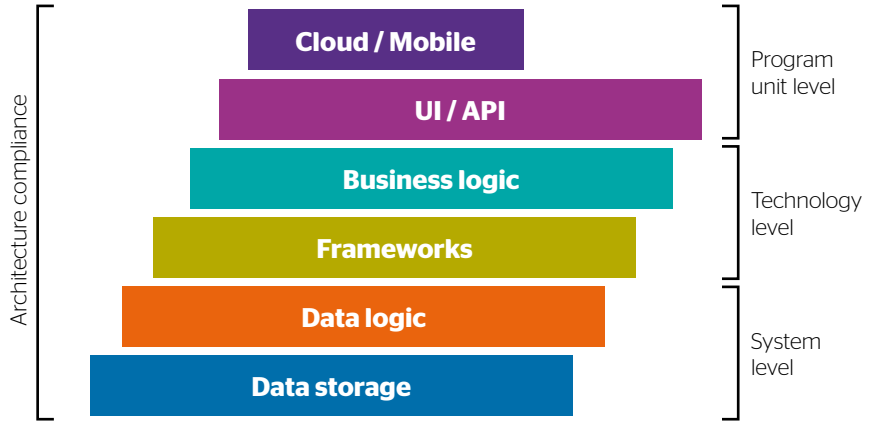


Architectural security

Because today's hackers have become more and more sophisticated, it's no longer enough to rely on firewalls and intrusion detection to protect the enterprise's most sensitive data. It is also well known among security experts that typically design flaws account for 50% of all security problems. We take a focused approach to secure software design by building security into the architecture in order to protect the most sensitive data first. When legacy systems are involved, CAST helps us parse the current architecture and find all the areas in the application that can touch sensitive data.

Once the secure design is in place, we use CAST to perform architecture-level checks across the technology stack of the target application. We build a set of custom checks that correspond to the design and we ensure to run these on our own development efforts. We also offer these checks to our clients as part of our solution delivery. Such checks might include separation of concerns, inter-layer dependencies, and traffic management.

Security across the technology stack



Innovation with CAST

Application portfolio analysis, powered by CAST

With a major part of the IT budget allocation being shifted from running the business to changing the business, application portfolio rationalization, transformation and modernization are key topics for CIOs in the next five years. Atos has developed a set of best practices to assess application assets and to identify improvement areas and migration paths.

Using fact-based KPIs from CAST Highlight's analysis – the CAST tool for application portfolio analysis – Atos can help customers implement a strategic plan to modernize legacy application landscapes. All the while significantly increasing IT agility and business value with a step-by-step journey towards 'liquid IT', where IT services flow dynamically to where it is needed by the business.

With the clear trend toward sourcing applications in Software-as-a-Service (SaaS) models from the cloud – or from an organization's own enterprise application store on a pay-per-use model – the threshold to migrating to a new application is greatly reduced.

Application cloud-readiness assessments

As more applications move to the cloud, IT organizations increasingly understand the need to evaluate an application's readiness for migration to the cloud. Characteristics of software, such as security, reliability, efficiency in resources usage, and architectural complexity, should be carefully analyzed. The consequences of migrating an application before it is ready can range from lost productivity, tarnished reputation, to serious financial losses.

Modern architectures that leverage web services and APIs present challenges in both the planning and execution of any cloud migration. The need to fully understand how different applications are dependent upon common shared services is more important than ever. Atos leverages CAST to clearly map each applications as-in architecture to pin-point critical and common dependencies, which enables our clients to effectively plan and phase cloud migration.

Combining CAST's deep structural analysis around application risk with our evaluation of the client's IT environment, Atos can provide a Cloud-Readiness Assessment of applications. The assessment not only helps organizations make smart and informed decisions about cloud migration planning, but also provides specific recommendations on how to prepare applications that may not be ready yet.

Proven enterprise architecture practices to support the migration

The activities to analyze the current application portfolio, the individual applications therein and the identification and implementation of improvement measures follow the proven methodology of TOGAF (Architecture Development Method). Atos has adopted TOGAF as part of the Atos Global Delivery Platform, which collects other industry best practices and reusables to ensure a consistent and streamlined approach towards migration projects. In each project there is a clear trace from the overarching business goals to the technical architecture, the implementation plan and the governance aspects, which helps to maximize the business value of the application landscape.

Driving innovation in software development

CAST helps to create that 'real world' view of the application by analyzing the structural properties, and thus by abstracting it into a model. Based on that model of the application, we can drive decisions on improvement areas as described before, and we can also create the foundation to drive innovation and improvements in the way the application is maintained or enhanced with new functional / nonfunctional elements. Model-driven development practices are used to create a direct link between the 'real world', the abstracted model and the application code.

Having the code directly linked to the model, and by driving enhancements of the application from that model together with automated code generation, not only can we greatly improve application quality and time to market, but we can also reduce cost at the same time. DevOps with the focus on automation, agile development, and continuous integration and deployment further supports this as well. Error prone tasks are automated, architectures are enforced and development iterations can happen faster. This allows our clients to see new functionality deployed faster, and helps them to focus investments on innovation.

Conclusion

An active approach to ensuring application code quality is crucial to successfully running a business, while keeping application lifecycle cost under control. By using the industry leading tools of CAST in combination with industry best practices and Atos expertise, Atos effectively empowers clients to make the shift to true digital business. The business technologists from Atos are the right partner for application quality control and management for the digital revolution.

CAST
ACHIEVE INSIGHT. DELIVER EXCELLENCE.

Atos

About Atos

Atos SE (Societas Europaea) is a leader in digital services with 2013 pro forma annual revenue of €10 billion and 86,000 employees in 66 countries. Serving a global client base, the Group provides Consulting & Systems Integration services, Managed Services & BPO, Cloud operations, Big Data & Security solutions, as well as transactional services through Worldline, the European leader in the payments and transactional services industry. With its deep technology expertise and industry knowledge, the Group works with clients across different business sectors: Defense, Financial Services, Health, Manufacturing, Media & Utilities, Public Sector, Retail, Telecommunications and Transportation.

Atos is focused on business technology that powers progress and helps organizations to create their firm of the future. The Group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and is listed on the Euronext Paris market. Atos operates under the brands Atos, Atos Consulting, Atos Worldgrid, Bull, Canopy, and Worldline.

For more information, visit: atos.net

About CAST

CAST is a pioneer and world leader in software analysis and measurement, with unique technology resulting from more than $120 million in R&D investment. CAST introduces fact-based transparency into application development and sourcing to transform it into a management discipline. More than 250 companies across all industry sectors and geographies rely on CAST to prevent business disruption while reducing hard IT costs. CAST is an integral part of software delivery and maintenance at the world's leading IT service providers. Founded in 1990, CAST is listed on NYSE-Euronext (Euronext: CAS) and serves IT intensive enterprises worldwide with a network of offices in North America, Europe and India.

For more information about CAST:

Web: www.castsoftware.com
Blog: blog.castsoftware.com
Twitter: www.twitter.com/OnQuality

For more information:
Please contact **dialogue@atos.net**