



## Doing Business Securely

## Application Security, what does it mean to you?

*Applications, whether they are web-based, service-oriented, client-server or stand-alone, implement the services offered by your organization. They determine to a significant extent your organization's interface to the external world. At the same time, these applications are the main entrance ports to your organization's valuable data for all sorts of users, including customers, business partners and employees. If you want to protect your services, secure your business and guarantee the confidentiality, integrity and availability of your data, you'd better take application security seriously.*

*In order to raise the security posture of your applications, you must deal with two major challenges: implementing appropriate and effective security controls, and meeting adequate security hygiene. Nowadays there is a focus on implementing security requirements by embedding these particular controls that are best enforced at application level (rather than at infrastructure or system level). The latter is about making sure to avoid vulnerabilities inadvertently introduced during development which would undermine the security controls that are embedded into your application, by ensuring the quality of the software that is produced.*

### Only few succeed

Unfortunately, experience shows that few organizations succeed in effectively producing secure applications in an efficient way. One of the main reasons is that software security is commonly thought of as pure execution of a penetration test at the end of the development lifecycle in combination with a penetrate-and-patch strategy after deployment. This is a big mistake, for two reasons:

- Two types of security vulnerabilities exist in software: bugs (implementation errors) and flaws (design problems). Statistics show that software, on average, contains an equal amount of bugs and flaws. Penetration tests are well suited for finding bugs, not for finding flaws.
- The cost of fixing a vulnerability depends on the time of discovery. Statistics, again, show that the difference in cost between fixing a vulnerability early in the development lifecycle or after deployment can be up to a factor 200!

Appropriate application assurance is a critical success factor when it comes to protecting your organization's critical information.

In many cases, the relevant laws, regulations and directives are not known, which could lead to criminal persecution, or denied compensation in case of a security breach.

### Application Assurance, an adequate solution?

Software development uses a multi-phase lifecycle, including activities such as design, implementation and testing. It is important to realize that many of the decisions taken during this lifecycle potentially impact the security properties of your software or applications. For instance, think about deciding on component interfaces during architectural design, which actually determines the number and type of entry points to your system.

### About Aszure

Aszure is specialized in operational risk management consultancy and staffing. Operational risk management, information security, business continuity and compliance to laws and regulations are major cornerstones of our services.

Aszure assists its customers with the incorporation of operational risk management at all levels and in all areas of their organization, including day-to-day operational decisions. No decision should be taken in any organization without applying proper operational risk management. It can be applied throughout the entire life cycle of any activity or project. In order to minimize risk, it is however preferable to apply operational risk management at the beginning phase of a project or operational activity.

### About Aszure Academy

Aszure offers, through the Aszure Academy, an extensive education and awareness program, covering several open classes, events and customized education experiences.

### Contact

For further and additional information, please contact us on Tel. +32 (0)9 243 10 20 or [info@aszure.com](mailto:info@aszure.com)

On all Aszure services our general terms of delivery apply.

Also the programming language chosen for implementation purposes can have a major impact on the security hygiene of your application (e.g., a safe language such as Java versus an unsafe one such as C). Application security necessitates a re-evaluation of these decisions from a security perspective.

*Application assurance* is a systematic approach to achieve application security. It is concerned with taking security into account on every step of the way during software development, and as such, it is a process-driven approach to application security. Application assurance will enable you to fine-tune development activities and to enhance your development lifecycle for security purposes.

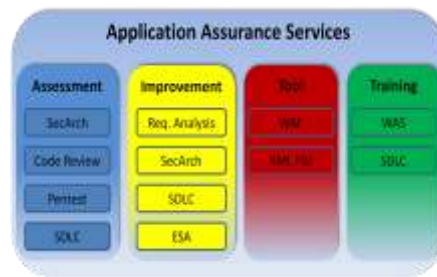
### Organization-wide benefits

A systematic approach of application security will provide you two main organization-wide benefits.

1. Reliable and stable software by controlling the introduction of vulnerabilities and flaws in your software. You will gain assurance that security controls are properly designed, implemented and continuously monitored in your software systems.
2. Cost reduction by anticipating potential security problems and by addressing them with minimal wrinkle effects. As such, it will enable more efficient development efforts, in line with the risks that you face.

### Application Assurance Services

Ascure offers several assessment and improvement -, tools - and training services for application assurance, guided by standards such as ISO/IEC 2700X, COBIT, the OWASP Top Ten, and the Common Criteria for Security Evaluation.



### Application Assurance Assessments

Assessments provide a focused way of measuring the security quality of your organization's development efforts. Not only do they pinpoint specific problems to be addressed in order to achieve an adequate level of security, they also give insight in the overall quality of your development efforts and, as such, they provide a very interesting software security metric.

Specific assessment services offered by Ascure include [security architecture review](#), [code review](#), [penetration testing](#) and [software development life cycle \(SDLC\) assessment](#). If you're looking for a truly meaningful security metric for your software, we advise the combination of three types of assessments: a black box software assessment (i.e. taking an attackers' perspective on your software, e.g. via a penetration test), a white box software assessment (i.e. taking a developers' perspective on your software, e.g. by means of an architecture review or a code review) and an SDLC assessment (e.g., based on maturity models such as BSIMM or SAMM).

### Application Assurance Improvements

Our improvement services focus on the execution or coaching of development activities for secure software. We focus on the early phases of the development lifecycle to enable a maximal return-of-investment of the consulting services.

The purpose of the [requirements analysis](#) service is to define a prioritized set of business-driven, measurable security requirements to be used for your secure software development effort. In [security architecture](#) improvement, the software architecture of your application is studied, fine-tuned and optimized for security purposes given the constraints of your development and production environment. [SDLC](#) improvement enhances your development lifecycle through the definition of appropriate process add-ons by combining the best of state-of-the-art models including Microsoft's SDL and McGraw's Touch Points. [ESA](#) improvement focuses on your organization's enterprise security architecture -an important enabler for application security- from a SABSA-inspired business-driven perspective.

### Application Assurance Tools

Product independence is an important value of Ascure, which allows us to provide our customers with advice that is not driven by internal sales strategies. In the domain of application assurance, application firewalls are important as they provide protection complementary to the typical software security controls. For this reason, Ascure offers its customers support in a trajectory of designing, selecting, deploying and maintaining [web application firewalls](#) and [XML firewalls](#).

### Application Assurance Training

Ascure training and awareness services for application assurance focus on [web application security](#) and [secure development lifecycle](#) training. In these one or two-day trainings, theory and practice are combined to get a solid understanding of the domain. Both trainings are offered in open classes or a customized education experience tailored to the environment, needs and requirements of your organisation.

Interested in world-class education and training on web application & services security: visit the website of the Ascure Academy ([www.ascureacademy.eu](http://www.ascureacademy.eu)).

For more information, please contact:

Tel.: +32 (0)9 243 10 20

E-mail: [info@ascure.com](mailto:info@ascure.com)

[www.ascure.com](http://www.ascure.com)

Bijenstraat 16-17, B-9051 Ghent , Belgium