

Security

Data Privacy and Independent Audits

## Data Privacy and Independent Audits

Let us first distinguish between data and information. Given that data is considered the building block of information, protection measures must be constructed at an equivalently high level for data or they will fail to provide the necessary level of protection. An accurate breakdown of layers, proper identification of safety requirements for each layer, and a thorough inspection of these measures are crucial. These layers can be devised unique to application, database, system, network, or the topography of your company. There are many options for logical division including development environments and subnet sets.

The maturity level in control processes is equally important. It is the layer that makes perhaps the most difference in service quality and security.

We classify control processes as follows:

- Internal controls and tests;
- External controls and tests;
- Standards;
- Governance systems, life-cycles, control points.

A realistically designed information safety life-cycle should also include company-specific check points. Then, you have to ask: Are these controls working? Are there any supervising structures in place? Are these controls assessed based on the principle of a separation of powers?

If you don't hesitate to respond with a "yes" to each of these questions, then we have a couple more questions for you...

Are the life-cycles in compliance with a defined disciplinary structure (ie. ISO 27701)? Are the definitions, instructions, and policies required by these standards in place?

If you're continuing to answer "yes," we are doing just fine.

Now comes the external specialist to inspect and verify your defined policies and practices.

## **Independent Audit and Reviews**

Independent review refers to the separation of powers in a corporate structure. For an external audit to operate effectively and efficiently, it must cover the following steps.

- Audit scope,
- Audit competency,
- Symptom management,
- Symptom removal,
- And verification.

Regulations, and the laws and agreements that dictate company services, will set the basis for the audit scope. These audits may include better-known disciplines including PCI and OWASP10 as well as code security, system infrastructure security, application security, IDOR tests, and penetration tests.

## **Next4biz and Independent Audits**

We have previously mentioned that maturity of control levels is the main layer in service quality and safety. The main determinants raising the levels of maturity are the independent audits and reviews.

As next4biz Information Technologies, we carry out periodic internal audits in compliance with our information security management system and work with specialized information security auditing firms.

Test methodologies for each layer,

- IDOR perspective for each environment,
- Structure of each environment,
- Security of each platform,
- System/Network infrastructure,

- And audit scope.

Once these have been well-established, we test for each layer, manage our findings, and validate them through independent sources. We consider integrated security the most crucial component of quality.

We conduct penetration tests, static code analysis, and logic tests to the software we develop.

We have obtained the ISO 27001 and ISO 27701 certificate through independent audits for our efforts to develop, implement, and continuously improve a Information Security Management System (ISMS) and Privacy Information Management System (PIMS). As these certificates indicate, we offer our customers high quality services in the field of information security.