



CIO Platform Nederland

Het CIO Netwerk van Nederland voor CIO's en ICT eindverantwoordelijken in grote organisaties

Information security



CIO Platform Nederland

Factsheet Member benchmarking

CIO Interest Group Informatie Beveiliging

CIO Platform Nederland
September 2010



BMTool - Information Security Benchmark Tool

With CIO-Platform Nederland's/Qubis' cross-platform Information Security BMTool, you can get a complete overview and benchmark of your information security policies in no-time. Your organisations' policies are benchmarked against the widely used ISO 27002 information security standard (or norm) as well as benchmarked against your branch members. The integrated delegation functionality allows you to address any question to your companies' experts. This ensures the benchmark is based on the most accurate and up to date methods applied in your organization.

Benchmark against the ISO/IEC 27002 norm

With information security being a hot item, security policies have earned a place high on the agenda at most companies' boards. The most applicable information security standards are the ISO/IEC 27002 norm - issued by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) - and *Control Objectives for Information and related Technology* or COBIT standard. These norms allow benchmarking the *codes of practice for information security management*.

Score your organisation using COBIT

Best practices have been gathered and combined in the *Control Objectives for Information and related Technology* (COBIT) and bright minds have developed the *Capability Maturity Model* (CMM). The COBIT complements the ISO 27002 norm: the COBIT covers a broader area, while the ISO 27002 norm focuses on security.

Use CMM

The questions that always arise when somebody mentions benchmarking are the following: are you sure you cover every aspect of information security? How are you going to measure all the aspects involved? While we already could answer the first question positively, we needed to give the second question some thought, and came up with CMM.

The CMM defines five levels or states your organisation could score in a certain situation. CIO Platform/Qubis transformed the COBIT and ISO 27002 standards into a statement set that can be answered using the CMM. This ensures you benchmark against all the facets of information security deemed relevant by the biggest authorities in this field. Visit www.cio-platform.nl for more information.

Form an industry

Organisations from within the same industry can combine forces by forming an industry ("branche in Dutch"). This has several advantages:

Set a BaseLine

In consultation with the organisations of his branch, the branch manager is able to set a benchmark BaseLine. The BaseLine contains the desired CMM level for relevant statements, and reflects on what good policies are. This ensures you will not only compare yourself with the best available standards, but you will also use the best available knowledge specific to your situation.

Learn from members and colleagues

Why reinvent the wheel, while you can also learn from your fellow members and colleagues? Within your branch and using the branch BaseLine, your branch manager can create reports that are specified up to the chapter level - all organisations being aliased to ensure privacy.



Create your own information security BaseLines

Your specific situation might justify a statement set that emphasizes a certain area within Information Security. BMTool supports this through the function of designing your own statement sets or BaseLine. You are able to benchmark your own organisation against your own statement sets.

Work...

...secure

Designing a tool for benchmarking Information Security policies brings an extra responsibility: the tool has to be *absolutely secure*. All local files are encrypted using SHA2048 encryption. The users' email address, mobile phone number and CIO-membership are verified before the tool can be used. Besides your password, text message verification is necessary for any action that changes files server side. Safety standards ensure secure communication between the central server and the Bmtool client. Your password is always necessary for accessing your encrypted local copy.

...wherever you want

You can work at any work station. With your copy of BMTool and encrypted user files installed on a portable hard disk, USB stick or CD, you can execute the BMTool program files anywhere you want. Furthermore, all your actions are saved automatically to the central server location. Upon logging in with your user credentials, BMTool will download the latest version of your user file.

...with whom you want - collaborate

Collaborate with your colleagues and organisations' experts or specialists. Delegate certain questions to the experts on subfields. Just give them a -free- User account for BMTool and request them to answer the statements you select for them to answer. Collaborating with your organisation is essential. With your licence, you get an unlimited number of licences for Users¹.

... always up to date

Upon logging in, your BMTool receives the latest version update or statement set updates automatically. Any norm extensions or updates are implemented with the least amount of hassle for you.

...work!

With integrated and automatic proxy support, we did our best to make our application as lean for your IT specialists as possible. If you have the rights to execute bmtool.exe and have 30Mb of permanently writeable disk space -whether on your hard disc, network disc or USB stick- and firewalls allowing this application to use port 80 and 443, the tool should work right away. If you still encounter problems, you can contact support for additional help.

¹ Users are able to give answers on statements. They cannot create statement sets, delegate their statements or do any task designated for Organisation Managers or Branch Managers.



Reports

Benchmarking without generating reports makes no sense. In fact, the reports are essential in the benchmark process. They indicate how well you do in comparison with the BaseLine, members and colleagues. BMTool therefore offers a variety of report presentations:

- Box plot view
- 'Traffic light' view - colours indicating how well you do.
- Copy-paste output - for use in your own reports.

More report possibilities will become available in the next version of BMTool. What the possibilities are? Have a sneak preview at only some of the planned introductions:

- Spider diagram view
- Time line view
- Bar diagram view
- List view

Advantages of BMTool:

- Benchmark against the combined COBIT and ISO/IEC 27002 standards.
- Use the proven Capability Maturity Model (CMM) to score your organisation
- Form branches
 - o Set a BaseLine for your branch in consultation with your branch manager
 - o Learn from other members of the CIO Platform and colleagues
- Create your own BaseLine for in-company benchmarking
- See your progress by periodical measurement
- Work
 - o Secure
 - o Wherever you want
 - o With whom you want
 - o With up to date software and statement sets
 - o With as little as hassle -and thus overhead- as possible

CIO Platform Nederland/Qubis

Why do CIO Platform Nederland and Qubis work together? It all started at the StrICTly for Business event, held by CIO Platform Nederland in 2009. One of the members of the group that won the competition, started IT firm Qubis with two fellow students. Nowadays, CIO Platform Nederland and Qubis are combining their strengths to using state-of-the-art technology and the wisdom of all members of the Platform for generating this benchmarking tool.

More information?

If you would like more information about BMTool, please let us know! You can send your email to bmtool@cio-platform.nl. Already convinced? Go to <http://www.cio-platform.nl/bmtool> for immediate sign up and ask your CIO to sign the relevant documents.