

Callio SECURA 17799

Callio Secura 17799 is software that enables companies to comply with the **ISO 17799/BS 7799** information security management standard. Callio Secura 17799 provides organizations with a practical method for developing, implementing, managing and certifying an Information Security Management System (ISMS). It also allows organizations to carry out audits for other standards such as COBIT or verify compliance with legislation such as Sarbanes-Oxley (SOX) by importing their own questionnaires.

FUNCTIONALITIES >

Callio Secura 17799 is a complete, easy to use and comprehensive information security management tool which will allow you to:

- Verify your level of compliance with ISO 17799 (gap analysis);
- Compile an inventory of your company's most important assets;
- Define the structures and processes within your ISMS;
- Mitigate the risks to each asset;
- Define scenarios for the implementation of controls;
- Draft your security policies (over 50 examples);
- Manage your policy documents;
- Approve or reject documents awaiting approval;
- Make policies, standards and procedures electronically available;
- Customize questionnaires;
- Import/export questionnaires;
- Verify whether your ISMS meets the requirements for BS 7799-2 certification;
- Document and justify the application of the ISO 17799 standard's 127 controls to your management framework;
- And much more...

The **ISMS Management** functionality will allow you to define an unlimited number of ISMS. In this manner, each security perimeter or security environment can have their own

distinct characteristics, allowing for ISMS specific implementation strategies. Each ISMS, along with its work teams, can be created, defined, and administered independently. Furthermore, users can be granted access to the different ISMS, and assigned roles individually.

This functionality also allows you to:

- Manage threats, vulnerabilities and controls. The threats, vulnerabilities and controls contained in the ISO 13335 standard are included by default; however, you can add as many others that you consider appropriate.
- Manage various types of evaluation criteria, such as confidentiality, availability, integrity and legal compliance. You can also add any other related criteria that you consider appropriate, such as effectiveness, efficiency, compliance, reliability of information (as per COBIT)
- Customize the vulnerability, occurrence and criterion scales used during the asset evaluation and risk assessment processes.
- Create associations among various types of assets, threats, vulnerabilities and controls. This will make it easier to manage and evaluate the ISMS and to implement controls designed to mitigate the risks to assets. The risk analyst can decide to deactivate these

relationships in order to work with all possible relationships among assets, vulnerabilities and threats. This enables the risk analyst to then develop a specific risk mitigation plan for an asset in particular.

The **Gap Analysis** functionality (in the Data Collection section) enables you to perform a diagnostic of your company or organization's current situation through the use of a series of questions or questionnaires. A standard questionnaire based on ISO 17799 controls is provided. This questionnaire can be customized and answers to the questions can be predefined and weighted. It is possible to incorporate and use questionnaires from other methodologies or standards that are based on best practices. You can also create your own questionnaires in order to carry out various audits. Entire questionnaires or specific sections or questions can be assigned to one or more users. When more than one user answers a question, the different answers are displayed, making it possible to assess the level of disparity among them. Questions can be adjusted in order to assign a higher value to some of them based on criteria set by your organization.

The **Risk Management** functionality enables you to evaluate the existing risks to each asset based on information about the organization's situation. This functionality also allows you to develop a risk mitigation plan. This is done by creating and evaluating different scenarios for the implementation of appropriate ISO 17799 controls, as well as any customized controls that have been added by the organization. This process makes it possible to determine

the best risk-mitigation solution for the organization, based on its risk management objectives and the cost of implementing the control or controls in question.

The **Audit Preparation** functionality enables you to do the following:

- Perform an ISMS diagnostic that will enable you to verify whether your ISMS fulfills the necessary conditions for BS 7799-2 certification.

- Generate a Statement of Applicability that provides justification for the applicability or non-applicability of each ISO 17799 control to your ISMS. The Statement of Applicability is required as the last mandatory step leading to BS 7799-2 certification.

TOOLS AND ADDITIONAL FEATURES >

Callio Secura 17799 includes various tools to help organizations with information security management.

These essential tools are as follows:

- A **Document Management** tool that enables you to meet ISMS documentation requirements by centralizing policies, procedures and other relevant documents while at the same time ensuring their distribution and control. This tool includes a document approval system, as well as a directory structure that allows you to organize various types of files. Using this tool you can control access to documents and manage version control. Over 150 templates are included to facilitate the project, including a range of security policies covering all sections of the ISO 17799 standard.

- A **Reports** tool to generate a number of reports automatically.
- A **Glossary** to help users understand the meaning of various information security terms.

In addition to the above characteristics, Callio Secura 17799:

- Calculates risk.
- Is available in English, French, Chinese and Spanish.
- Contains an Awareness Centre portal for the distribution of approved policies. These policies help raise staff awareness regarding information security issues. Staff member roles and functions within the organization determine the policies to which they are allowed access. Using the Document Management tool, documents can be published to the portal after

having been approved. Publication enables documents (generally policies) to be made available to Awareness Centre users with specific predefined profiles or roles;

- Includes an online Help system;
- Is a multi-user, Web-based application that does not require the product to be installed on individual user workstations who will access the software or the organization's approved policies.

SYSTEM REQUIREMENTS >

SERVER REQUIREMENTS

Computer	IBM® or compatible (800 MHz and greater)
Random Access Memory (RAM)	512 MB
Disk Space	1 GB (minimum) 2 GB (recommended)
Network Adapter	100 Mbps
Operating System	Windows® NT, 2000, XP or 2003
Database	MySQL or SQL Server
Web Server	IIS 4/5/6 or Apache® 1.3.x / 1.2.x
Software	New Atlanta® - BlueDragon® JX Server

CLIENT REQUIREMENTS

Computer	Windows®-based personal computer
Screen Resolution	800 by 600 pixels or higher
Web Browser	Internet Explorer® 5.x, 6
Software	Word processing software