Main Features of Mawida Good Practices

Introduction

The present work enumerates the main features of the tool Mawida BP to show, in broad terms, its potential.

General Description

Mawidabp is a system with features for the administration and management of good practices, allowing organizations to constantly improve their processes in an agile and ordered manner.

The application is developed in a Web environment, so there is no installation process, and it can be accessed from any browser that fulfills W3C standards.

The system provides access controls to the information by levels of authorization. It enables the creation of user profiles according to the person's role in the organization.

Moreover, every action performed within the system is stored, registering what changes were made, who made them and when, and allowing you to trace those procedures.

This is a system developed under the best programming standards and design patterns, guaranteeing the best resolution for each process and achieving a robust, scalable model.

Uses

This tool Works perfectly in any area or department of a formal organization (with defined processes and good practices) that, within the framework of a predefined plan, carries out different kinds of evaluations to detect deficiencies or opportunities for improvement that demand a remedial action plan.

The tool manages the following cycle in its entirety:

FORMAL ORGANIZATION

This means the feature covers the full cycle: from the upload of Good Practices, through business processes, to the control objectives. Moreover, it foresees the generation of a work plan, and then it integrally manages its execution.

Main Functions

Functions at user level:

- Integrated Security enables you to use the hierarchies defined in Active Directory, which is correlated to the visibility or interaction in the improvement opportunities.

- Planning: integral, complete administration of the work plan, identification of possible delays, etc.

- Efficient administration of online paperwork.

- Integral WorkFlow:

    - Durante la execution of the Audit: from the origin of the issue to the obtaining of an answer.

    - During the Follow-Up: facilities such as an automatic calendar, a calculation of input time, configurable delay alerts, etc.

- Full web, compatible with portable devices. It can be installed in servers hosted by Cirope S.A, or in servers managed by Customer System Management.

- Collect preexistent observations and link improvements opportunities.

- Surveys (with a view set on a QAR).

- Management of resources' costs.

- Unique view of the observations, with all "incentives" together in one place.

- Work is done fully online, by both the auditors and the auditees (the "observation" becomes more important than the "brief" document).

- Process Integration: it eliminates additional computations to obtain the Internal Control assessment of the processes or of the Functional Units.

- Eliminate e-mails with attachments.

- Corporate consolidation of good practices.

- Possibility to automatically grade audits and to standardize assessments.

- Better deadline achievement.

System Features

System administration

It allows you to manage the system. Establishing a proper configuration during system set-up is fundamental to then be able to enjoy all the benefits that Malawida's functions provide.

Good Practices

In this section you can load the good practices (models, standards, etc.) that can later on be used in the briefs. Some examples of good practices are:

- COBIT
- COSO
- ISO 27001
- Any control authorities' regulations.
- In general, external or internal instructives that regulate processes.
- For every good practice, you have to establish the **Control Goals** for each **business process**. For every Control Goal there are detailed procedures that can be applied:
  - Design evaluation: established over the design of the controls; inasmuch as the design lets you trust the Entity's inner control, they must be tested (given that they can exist but not be applied properly).
  - Compliance tests: these determine whether the controls are fulfilling the objectives and actively working.
  - Substantial tests: performed to obtain audit's evidence in order to detect important misrepresentations on the financial statements. There are two types of these tests:
    - Details of transactions and balances' tests
    - Analytical procedures

Users

The system incorporates the native functionality of working with Integrated Security (Windows AD), but you can make changes to the users list.

Surveys

It includes the possibility of sending Surveys to the users of the system. This functionality is useful to detect the level of satisfaction of the internal client and, eventually, to plan its improvement. This is typically a job required in environments with some kind of Certified Quality standard.

Profiles and privileges

Each user has to have at least one **Profile** associated to a particular **Organization.** Each Profile specified in the system has a series of **Privileges** (permits) that will determine the access to certain system functionalities. The defined profiles have, in general, access to the following privileges:

Administration

Access to all system functionalities.

Security

Access to the organizations' management, with their business units (reading). Security reports and Profiles and privileges (reading). Handling of users (reading/writing). General system configurations (reading/writing/deleting).

Auditee

Access to relevant findings and notifications (Reading/writing). Solved or reiterated findings (reading). There must be at least one user with this profile in each one of the audit reports, and in their respective findings.

Auditor

Access to business and users' units (reading). Handling of good practices (reading/writing). Resources and periods (reading). Management of the audit programme (reading/writing). Execution Reports. Execution and work programs briefs (Reading/writing). Observations, opportunities for improvement and control goals (reading/writing/deleting). Draft report (reading/writing/ deleting) and final reports (reading/writing). Notifications and pending findings (reading/writing). Findings that were solved or repeated (reading). Audit reports. There must be at least one user with this type of profile en each audit report and in their respective findings.

Supervisor

Access to organization's management (reading/writing). Business units ((reading/writing/deleting). Users and e-mails (reading). Handling of good practices (reading/writing/deleting). Questionnaires' reports. Complete access to Planning, Execution and Conclusions. Pending findings and notifications (reading/writing). Findings that were solved or repeated (reading). Follow-up reports. There must be at least un user with this profile in each one of the audit reports and in their respective findings.

External Auditor

Access to Execution briefs, observations, improvement opportunities, controlves (reading). Final reports (reading). Pending findings (reading). Findings that were solved or repeated and notifications (reading).

Comitee

Access to good practices (Reading). Questionnaires' reports. Planning (reading). Final reports (Reading). Executions, Conclusion and Follow-up reports.

Written off

It doesn't have any privileges within the system.

Audit Planning

In this section the annual tern-planning is defined, allowing the assignment of human resources, supplies and their costs. As a result, you get the estimated cost of the project (material and human) of an audit and by **Audit Plan.**

Resources

It allows the definition of resources that are grouped by class, for example: housing, personnel, mobility, etc. These will, later on, be available to be assigned to the **Plan** and **Work Programme** of the audit.

Periods

In this section you must define the **beginning** and **finishing** dates that will determine the period in which the audits will be planed.

Work Plan

It allows the management of the **Audit Plan**. In it you can establish the projects (audits) with their respective resources and time estimates. Each project belongs to a Period and a Type of Business Unit.

Audit Execution

During the **Execution** phase, the system reflects the process through the possibility of creating Reports for each one of the audits that have been predefined during **Planning.**

Briefs

A **Brief** is the presentation of the audited business unit during a certain period. This brief must have been included previously in the **Planning** of the audit

Reports

In this section you can acces reports with data based on Execution Briefs. There are two types of reports:

- Management summary: list of briefs with their own business processes and findings grouped by Type of Business Unit.
- Complete report of findings by brief and state: summary of all the findings made, detailed by the state where it is at, and grouped by brief.

Audit Conclusion

After the Execution of the audit, you must generate a Draft Report (which corresponds to the Report created in Execution and that, at the same time, was defined in Planning) to subsequently be able to generate the Final Report. Asides from facilitating the delivery of reports, this module provides reliability over the content, since it is not possible to alter it once the Final Brief is issued.

Audit Follow-Up

From the moment when the **Final Brief** is issued, the **Follow-Up** stage begins, where we can see the development of the findings. Each user will have access only to the findings to which he is related to (he may be the owner of the process or be related to it indirectly). Here you can find pending and solved findings