antares

White paper

[antares RiMIS® ICS - Internal control system

[Introduction

The purpose of this document is to describe the functions of the ICS extension module for the antares RiMIS® risk and opportunity management software.

antares RiMIS® is a software for opportunity and risk management. Elements of this standard software are action management and reporting, as well as Monte Carlo simulation and risk identification by means of questionnaires.

The software is primarily designed for industry, service and trade, corporations, joint-stock companies and larger medium-sized businesses.

Thanks to the complete documentation of process controls, as well as workflow-supported monitoring, antares RiMIS® ICS ensures through effective procedures that your business processes run transparently, securely and according to defined (legal) regulations. The procedure covers all corporate bodies, including the supervisory board and the management.

The ICS module is available from version 3.7.2, which was released in September 2012. This module is not part of the standard license for antares RiMIS® and must be licensed separately.

[1. Purpose of the module

An internal control system (ICS) is used for software-supported internal process control and the documentation and monitoring of business processes in companies. It also provides protection against and prevents acts of abuse and damage within the company.

The main objectives of the ICS include monitoring and preventing risks, ensuring the functionality and efficiency of business processes and the reliability of operational information, as well as safeguarding assets. Extensive control measures and complete documentation prevent material misstatements in financial reporting and ensure complete and correct accounting records. To achieve these goals, antares RiMIS® ICS relies on various principles, such as transparency and minimum information.

Organizationally, the monitoring of controls should be closely coordinated with the monitoring of other risks not inherent in the process. Since antares RiMIS® is web-enabled, any number of people can access the system decentrally and thus consistently participate in the process or independently obtain information.

[2. Definitions

2.1 Process

A business process is an essential procedure in a company. For the ICS module, a process or sub-process is the key element for the assignment of controls. A process can consist of any number of sub-processes. A sub-process occurs only once and only once within the process structure. The process structure can consist of up to 15 levels. There must be a summary node under which all processes and sub-processes are listed ('All business processes' or similar). If a similar subprocess exists in different processes, it must be ensured that this subprocess is unique, e.g., by means of a unique ID or a unique name. This is the only way to ensure that individually different controls can be addressed to a sub-process.

The process description and the process structure can change at any time, i.e., changes should be traceable (history). The process description can be recorded in several languages. A process has a unique, alphanumeric ID. A process cannot be deleted due to the historicization, only deactivated. The assignment between process and subprocess is also historicized, consequently also only deactivated.

2.2 Legal entity

A legal entity is an organizationally largely independent unit and an independent legal person. Legal entities can in turn be combined into a legal structure. Shareholding relationships are currently not recorded in antares RiMIS®. In addition to the legal and process structure, it is also possible to map an organizational structure in antares RiMIS®. In the legal structure, non-independent units, such as production plants, can also be classified hierarchically. Individual units can also be combined into a regional structure using summation nodes.

2.3 Assignment between legal entity and processs

In antares RiMIS® it is defined for each legal entity which process in the legal entity is to be regarded as its essential process. The standard checks and the form in which the checks are to be carried out are derived from this later. The assignment can be made on several levels (e.g., must/ want/nice to have/ not relevant).

2.4 Damage potentials

A process can have several damage potentials, which are synonymous with potential risks. The assignment to predefined standard risks serves to integrate the ICS into the standard risk management process and is intended to facilitate the recording of controls and further measures. A damage potential consists of a unique ID, a description, which can be multilingual, and a flag, depending on whether the damage potential is a mandatory damage potential (derived from the process) or not. From individual risks, further damage potentials can be created via a standard process within antares RiMIS®.

2.5 Assignment between process and damage potential

A process or sub-process can be assigned several damage potentials. A damage potential can also be assigned to different processes.

2.6 Control target and assignment to control

The control objective is to define what the objective of the controls is with regard to a process. One or more control objectives are assigned to a process. A control objective can be, for example, validity (of the data) or security. Control objectives and their assignment can only be created centrally and company-wide. A control objective is used to test the effectiveness of the controls at a later date.

2.7 Controls

A control consists of a title, a long text description and references to external documents, such as a management manual, all of which can be created in multiple languages. In addition, a control has the attributes target frequency, target check frequency, type of control, documentation obligation and the distinction as to whether it is a standard control that is a top down specification or an individual control that is created by the decentralized ICS manager. Furthermore, it is defined whether the control is mandatory or voluntary. This requirement can be made stricter in individual cases, but no relief is provided for legal entities that are required to perform controls via process assignment.

2.8 Assignment between process & control

The process ultimately determines the damage potentials that exist in a legal entity as an organization and how these risks can or must be countered with controls. On the one hand, this is defined by a top-down specification on the part of the Group; and, at the same time, individual risks can also be countered with controls that the risk manager defines and designs for themselves. This assignment represents a 'target specification' that is anchored in the legal entity's personnel.

2.9 Assignment between control, legality and process

From the aforementioned target specification, the concrete responsibility is derived as to which person (and representation) is technically responsible for the control, in which form the control is actually carried out, as well as how and where the concrete control is described further.

2.10 Execution of the control

The documentation of the execution of the control is to be made according to the control frequency and proved by uploading a document.

2.11 Implementation of the control effectiveness test

The effectiveness and traceability of the checks must be reviewed periodically in accordance with the control-check frequency. This can be evaluated on several levels and presented in more detail with a free text.

2.12 Multi-eye principle, documentation

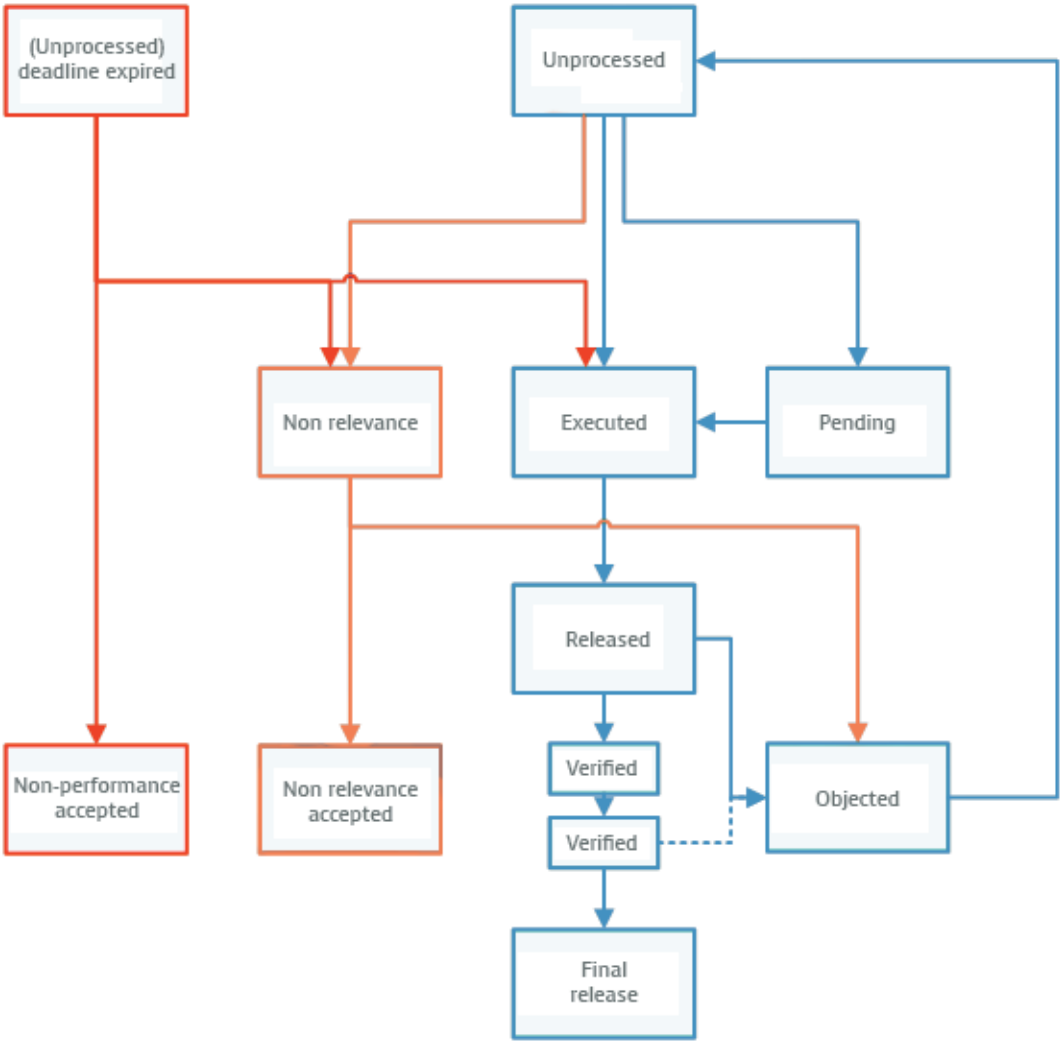
The execution of a control is signaled by an automatic process to the control manager (usually the CEO), who monitors the execution. This multi-eye principle can be carried out via a release process covering up to 15 stages.

2.13 Control frequency

Controls must be carried out periodically on a regular basis. This is recorded centrally in the control's master data. The control frequency is used to calculate when the control must be carried out at the latest, e.g., if the frequency is once per quarter on 31/3, 30/6, 30/9 and 31/12 of any given year. If a control is not carried out within this period, this must be justified and accepted by the ICS manager, for which a separate status is provided.

[3. Control workflow

The controls should be carried out periodically depending on the specification. The workflow process is provided as follows:



- After each period, the control is set to the 'unprocessed' status.

- A control can be edited (change of control comment, change of document attachment) until it is released ('Approved'). As soon as the approval has been granted, no more changes can be made to the control comment or the file attachment.

- Rejection of the control ('Objected') requires the entry of a comment by the rejector. Afterwards, the control can be edited as desired until it is released again.

- The release process 'Verified' must go through every instance of the ICS ICSM structure. A rejection can occur between releases, in which case the control is again directly with the controller.

- A 'collective release' can be made for the release steps, several controls can be marked as 'Verified' in one step.

- Controls can be marked as 'Not relevant' by the control manager, which has to be done again every control period and has to be accepted by the direct superior in the approval process.

- If controls have not been performed in a control period, they are continued as 'Not performed' in the current period. The control can be performed afterwards or the next position in the release process accepts the non-performance.

The controls to be performed are displayed in a filterable/searchable and sortable overview screen. Here, only the checks that are to be performed by the logged-in user are displayed. Specific options are offered via a context menu. This non-exhaustively includes: Execution of the control (via dialog mask), detailed information about the control (via dialog mask). A different view of the overview screen is used to display the controls to be checked. The sorting in turn ensures that the currently pending tests are mentioned at the beginning of the table. For the respective status it can be parameterized as to whether a document or comment is necessary.

[4. Risks and controls

antares RiMIS® already provides a comprehensive measure management with status monitoring of the measures, examination of the efficiency of a measure and semi-automatic derivation of the net risk evaluation. Measures can be typified in different ways, e.g., emergency planning, regular maintenance, one-off activity. In this context, a control represents a kind of preventive measure to be carried out on a regular basis. However, the special feature of a control is that for each legal entity, it is specified in a top-down process which controls are to be performed, which depends on the business processes that exist in the legal entity and are more or less pronounced.

These specifications result in 'Mandatory risks' and related controls. In addition to the execution of the control, the risk must also be individually described, evaluated, etc., but this will not be discussed in detail here. The top-down predefined controls can be supplemented with individual controls by the risk manager as desired. In addition, other measures can be defined that are not controls.

[5. Individualization of controls

Decentralized entities have the possibility to individualize individual controls in the following ways:

- Tightening of the necessity to perform a control (e.g., from optional to mandatory).
- Comments on the control, e.g., how is a control actually carried out/implemented/documented at the subsidiary?
- Increasing the control frequency, e.g., from once per quarter to monthly.
- Display whether a control is performed automatically by a system (reference to the system) or manually.

[6. Top-down specifications

6.1 Definition of the processes

A centrally responsible ICS manager defines which legal entity implements which of the various processes and thus controls. In both the process and the legal structure, the definition is inherited in the case of multi-level hierarchies, so that the maintenance effort is kept as low as possible. The implementation obligation definition itself can be multi-level (mandatory process, possible process, etc.).

6.2 Definition of control managers

Control responsibility must be defined manually for each legal entity, whereby different persons responsible for each control can be defined for each organizational unit, legal entity and process. In addition to the manager, a substitute can also be provided for. The person assignment can be defined either in a centralized or decentralized manner, e.g. by an area manager. The specification of which controls are to be carried out by which control manager is carried out via a central administration mask. This mask is also available to decentralized managers in subsidiaries/companies, who can define the responsibility for their respective authorization.

6.3 Definition of the ICS owner/ICS manager structure

For each combination of legal entity, organizational unit and process, an ICS manager can be assigned for each ICS owner. The legal/org/process combination does not have to be at the lowest level, but can also be a node that is in turn inherited by all subordinate nodes. With this assignment, the input is facilitated by a multi-selection. This assignment ultimately determines which ICS manager is responsible for overseeing the implementation of the control.

6.4 Definition of controls for processes

For each process, any number of controls can be selected and assigned to be obligatorily performed by the controller in a legal entity.

6.5 Damage potentials to processes

For each process, different damage potentials can be created, from which risks can be derived. A damage potential can be given the characteristic 'mandatory risk'. By definition, these risks are present in every legal entity assigned to the process (see 5. a) and must be periodically assessed and released. Controls result from the assignment of the risk to this process.

[7. Effectiveness test

At regular intervals (control check frequency), which are defined for each control, controls are to be reviewed for their effectiveness, traceability and target fulfillment. Another overview screen is used for this purpose. The effectiveness and traceability can be assessed in different classes. In addition, comments can be captured during the review. The objective of the effectiveness test is a periodic review of the controls to determine whether they are having a positive effect on the control objectives and thus counteracting the underlying risk.

[8. Evaluations

Evaluations are already delivered with the standard system:

- Overview of performed controls, controls in delay, controls hanging in the release process with drilldown possibility.
- Aggregated view from process, legal and organizational perspectives (number of controls by priority, status, number of controls requiring documentation, etc.).
- Effectiveness evaluation: Presentation of efficacy evaluations. In addition, it is possible to jump to assigned controls at various points within the risk evaluations in order to check their status and obtain detailed information.

[9. Notification

antares RiMIS® already offers numerous event-driven notifications, which are extended by the following notifications for the ICS:

- Automatic notification when the control date is approaching
- Automatic notification when the control date has expired
- Automatic notification when the control date has long since expired
- Manual notification function for contacting the control manager and the respective ICS manager. These notifications can be enabled/disabled by the administrator. Notification parameters, such as grace periods, are maintained centrally.

[10. Authorization and release process

The extensive authorization functions of antares RiMIS® are also used in the ICS area. In this way, users can be authorized for legal entities, organizational units and processes, and in turn, inheritance is made possible. In addition, one process, one legal entity and one organizational unit are defined per user for the default setting. The ICS release process differs from the risk release process, as there may be different responsible ICS managers for individual controls that a user has to perform. The distinction can be made in one or more structures, e.g., a different ICS manager may be responsible for the purchasing process than for the sales process, but the control may be performed by the same person.

[11. Report portfolio integration

For the existing report portfolio in antares RiMIS®, special versions of the evaluations are created, with which either an independent ICS report portfolio can be created or the ICS area can be integrated into the risk management report. This is the responsibility of the user who defines the report portfolio.

[12. Outlook

antares RiMIS® is constantly being further developed. Numerous suggestions for improvement from customers are incorporated into each new version, and the same applies of course to all extension modules. Further steps in the development of the ICS module could go in the following directions:

- Evaluate the costs and benefits of controls to assess efficiency and, if necessary, replace individual controls that are not legally binding with more efficient controls.
- Expand evaluation capabilities to facilitate experience sharing between different legal entities.
- Introduction of a proposal process to define standard controls from the individual controls of a legal entity.
- Expansion of decentralized admin functions.

antares

[Software for reliable decisions

[Software for reliable decisions

antares Informations-Systeme GmbH
Stuttgarter Str. 99
D-73312 Geislingen

Tel. +49 7331 3076-0

www.en.antares-is.de
info@antares-is.de