VERISCAN SOLUTIONS FOR HANDLING PERSONAL DATA AND MEETING THE REQUIREMENTS OF GDPR

White Paper GDPR solutions

White paper for Veriscan solutions for handling personal data and GDPR

Commercial White Paper

Veriscan
Publishing date: 2017-02-06
Minor language update: 2017-08-21
Publisher: Veriscan Security AB
Document ID: White paper
Version 1.1.2
Information class: Public

Table of content

Notes

ABOUT

This white paper targets people and organizations that are looking for tools and methods that support implementation solutions to meet the requirements of the new General Data Protection Regulation (GDPR) set forth by the European Union. It is written for commercial purposes to enable the market to utilize Veriscan solutions and tools for GDPR.

This white paper shall not be used as any reference for fulfilment of either the ISO/IEC 27001 requirements and/or the GDPR. For this purpose, the original standards and the GDPR apply.

Veriscan has been part of the standardization work within ISO SC27 since 2004 and acts as experts within information security primarily in Sweden but also in other countries. This paper is however not written for the situation in Sweden but has a more general approach.
The white paper is a presentation of Veriscan's expert view of how to go about to fulfil the requirements.

The presentation of Veriscan's own solutions, including products and services, provides examples of how the GDPR requirements can be fulfilled.

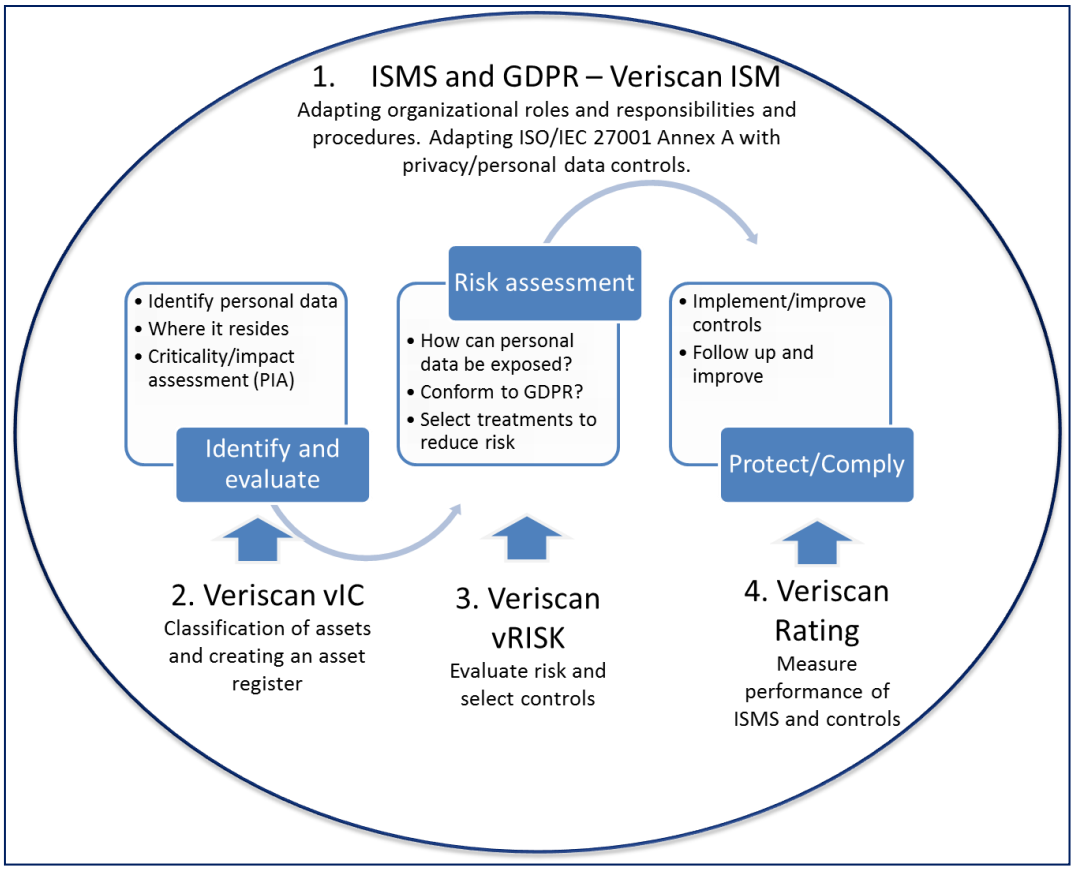
Note that the products presented are generic and can be used anywhere by anyone, while the professional services are customer specific.

This white paper can be seen as an extension of another white paper by Veriscan that provides information for organizations that have an ISMS according to ISO/IEC 27001:2013 and face GDPR regulations. It provides a base for the views and solutions presented in this white paper. For more information about the other whitepaper see www.veriscan.se.

CONTRIBUTORS

This white paper is written by Veriscan Security AB. The solutions presented herein have been verified by customers.

Abstract



This white paper further describes the connection between GDPR and information security (management systems), ISMS, as defined by ISO/IEC 27001 based upon Veriscan solutions.

Veriscan has been providing expertise and solution with information security in general and the information security management in particular for many years. Many of the issues raised by GDPR can be addressed by already existing information security processes in the organization and/or by support and tools from Veriscan.

The GDPR work should be performed as part of a structured approach to overall information and cyber security needs and by utilizing existing solutions. This approach may then result in less effort needed for GDPR and the effort done will have a long term effect and better efficiency.

In lay man words:

– Use what you got instead of inventing new things; or

- if you need to invent something - let's make it long term usable

Veriscan has divided the solutions in four areas or steps as seen in the central picture above (figure 1). This can be seen as a complete package but each step can be used separately depending on what the organization has in place. This white paper gives

an overview and more detailed information about the four steps and Veriscan solutions in principle:

1) Use the current information security management system to address GDPR – Veriscan ISM

2) Identify and know the value and where the personal data resides – Veriscan vIC™

3) Determine risks and protection by controls – Veriscan vRISK™

4) Evaluate performance as a basis for improvements and compliance evaluation – Veriscan Rating®

Obviously the second step is crucial for GDPR compliance as if the organization has not identified, valued and knows where the personal data is, none of the other GDPR requirements can be properly addressed!

1 Veriscan solutions in relationship to ISMS and GDPR

1.1 Introduction

This is a white paper of Veriscan Security, an expert organization in the area of information security. It presents Veriscan's view of the process to comply with GDPR as well as important requirements that should be met by any solutions selected to be used in the process.

This white paper gives organizations a set of solutions with tools and methods to start and complete the work to comply with GDPR by using solutions that also are applicable to an information security management system (ISMS) according to ISOI/IEC 27001:2013.

GDPR will impact all organizations' handling of personal data within the EU but most likely will also have a global impact as it covers the personal data of EU citizens regardless of by whom and where the data is handled. GDPR is addressing many important issues, such as:

- The definition of personal data has become broader including genetic, mental, cultural, economic and social information.
- The rules for obtaining consent have become tighter.
- Many organizations need to appoint DPO:s (Data Protection Officers)
- Privacy Impact Assessments have become mandatory
- Data breach notification within 72 hours after discovery.
- The right to be forgotten, i.e. organizations are not allowed to keep personal data for longer than absolutely necessary.
- Fresh consent is required when altering the use of personal data.
- Legal action against any organization regardless of where in the world the company is based and where data is stored and processed.

The connection between GDPR and information security (management systems), ISMS, as defined by ISO/IEC 27001 and the advantage of using an existing implementation of an Information Security Management System, ISMS, are generally and in more depths described in the White Paper – "Information security management system (ISMS) and handling of personal data".

1.2 Veriscan solutions overview

GDPR is by many organizations seen as an issue of its own. However the work required to comply with GDPR is bound to connect to many other processes, ICT systems and people in the organization.

Veriscan's approach to address GDPR is to view the issues as part of the overall information security. It doesn't mean an organization cannot comply with GDPR if they don't have an ISMS, but it will certainly be an advantage to have one.

An ISMS adjusted to address personal data according to GDPR is suited to manage the risk and identification process as well as the controls of GDPR. Veriscan's solutions are linked to ISMS in general and are flexible to handle various types of requirements e.g. to handle GDPR. This is shown in figure 1.

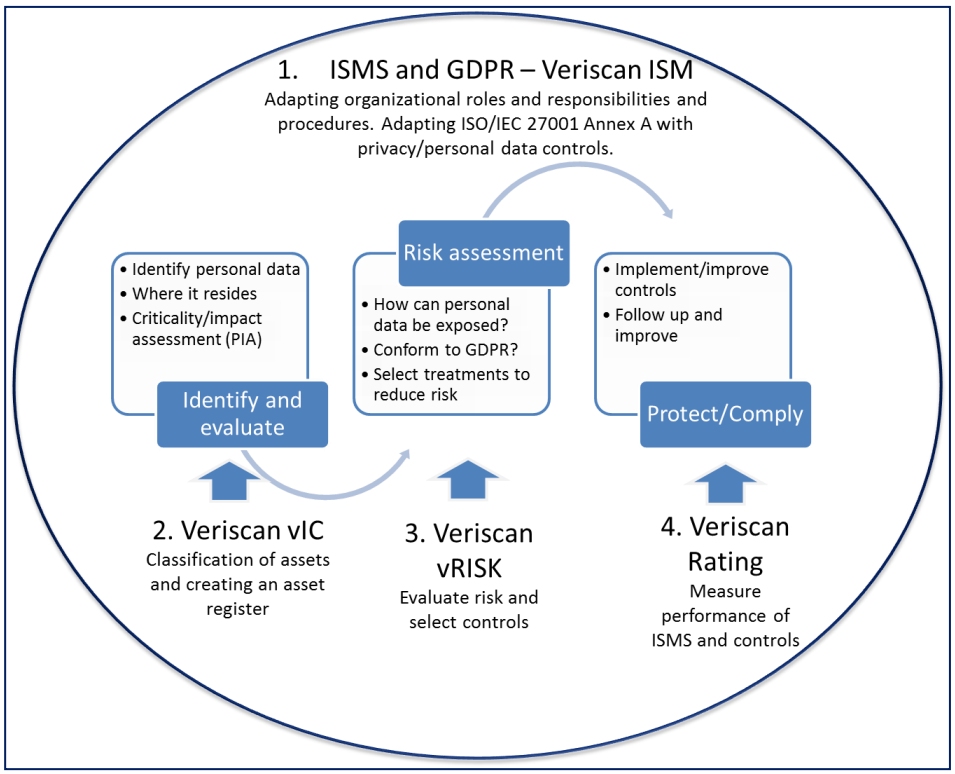


Figure 1 shows an overview of the main GDPR content (source Veriscan)

Figure 1 shows an overview of the main GDPR steps and Veriscan solutions in the context of an ISMS according to ISO/IEC 27001 (source Veriscan)

The following process describes recommended steps to be taken in order to comply with GDPR and relation to the figure above and Veriscan solutions.

1.3 The four steps and structure of this WP

The solutions required to successfully execute a process for fulfilment of GDPR supported by Veriscan are in this white paper concluded into 4 main steps as in the table below:

NOTE: It is possible to use the solutions of Veriscan as described in steps #1-4 separately.

STEP TO COMPLY	PURPOSE	VERISCAN SOLUTION
#1 Awareness & Acceptance for GDPR and ISMS	- Ensure that the organization understands the impact of GDPR to allocate sufficient resources to start and complete the work. - Ensure efficient utilization of already existing processes in order to avoid unnecessary costs and confusion. - Create a speedy adaptation to GDPR.	**Veriscan ISM** A consultancy service tailored to the need of the specific organization based upon standards (such as ISO/IEC 27001, 27002, 27003, 27018, 29100, 29151).
#2 Identify & assess by evaluating Personal data	- Identify what data to be protected - Perform Privacy Impact Assessment (PIA) - Identify where the data resides	**Veriscan vIC™** Supports efficient Information Assets classification from both an information and ICT resource perspective.
#3 Risk assess and determine treatment	- Assess the risks associated with the data - decide means of protection (To mitigate risks and comply with GDPR requirements on e.g. consent, transfer, breach notification, the right to be forgotten)	**Veriscan vRISK™** Supports efficient Risk Management across any organization and risk type.
#4 Evaluate protection and Compliance	To measure the performance for compliance with GDPR	**Veriscan Rating® - Veriscan vEAVER™** Support performance measurement of the level of protection.

This white paper is structured based upon the four steps above as follows:

- Clause 2 – describes step #1 - Awareness & Acceptance for GDPR and ISMS
- Clause 3 – describes step #2 - Identify & assess by evaluating Personal data
- Clause 4 – describes step #3 - Risk assess and determine treatment
- Clause 5 – describes step #4 - Evaluate protection and Compliance

There is sometimes a 5th step mentioned as “Protection”. This step is seen as embedded in the four steps. This as there is always a current state of both protection and need of protection that should be taken into consideration. To determine what personal data to protect and why, in combination with what protection already exists, is of course the most efficient way. Using all or some of the four steps will put the “protection” into the right context for each organization. It will also ensure that the GDPR work will have a long term effect and support the “privacy by design” objective.

1.4 How Veriscan solutions interact

Veriscan's solutions are closely related to standards and established best practices for information security, e.g. ISO/IEC 27001. In fact, Veriscan has provided the editor of the ISO/IEC 27003 implementation as well as for the guidance standard for implementing the requirements of ISO/IEC 27001 (ISMS). Veriscan has a fundamental understanding that these standards are written to be used for any organization. However, the use and actual implementation of an ISMS is often unique. This means that any solution provided must be adaptive to the unique situation of any business.

The conclusion can be described as; even if there are standards there are no "standard" solutions. The Veriscan solutions are based on experience and knowledge from working with various types of businesses. This enables Veriscan to support each individual case and to develop tools that are easy to adopt. In general, an effective ISMS must be able to support the overall business objectives.

Apart from the strict legal issues of GDPR, it is very much an information security management issue. Veriscan can help businesses to handle this issue in various ways that enable a better legal judgement and thus enable an efficient way of solving the overall GDPR concerns.

There are various methods and tool that can be used to support the processes of ISMS and GDPR.

The Veriscan ISM is not a tool by itself but a support for getting the GDPR work in the right context on how the organization will address the requirements in relationship to how they manage information security. There is always one way or another that the organization handles information security. It is a clear advantage if the GDPR work is integrated in other information security management processes. How this could be done is of course different from case to case. Veriscan experience and methods for information security management can provide proper awareness, understanding and planning of activities (as in step #1, described in clause 2 in this WP).

The Veriscan vIC tool supports the identification and valuation of information assets (classification) processes as part of an ISMS and can then also support these similar requirements in GDPR (as in step #2, described in clause 3 in this WP).

The Veriscan vRISK tool support the central risk management process in ISMS and can also support this requirement in GDPR. This should then also enable selection of controls and adjustment or additional controls as stated in ISMS (as in step #3, described in clause 4 in this WP).

How well the controls, organizational as well as technical, are compliant with GDPR and the risk appetite of the organization is a matter of the performance of the ISMS. This performance can be evaluated by measurements provided by the Veriscan Rating. Veriscan Rating is supported by measurement programs and a tool called Veriscan vEAVER that can be used to evaluate the performance of an ISMS including GDPR issues.

An important note to make is that Veriscan ISM is not a prerequisite for using Veriscan vIC, Veriscan vRISK and Veriscan Rating, respectively. Also, there are no dependencies between Veriscan vIC, Veriscan vRISK or Veriscan Rating as they can be used separately.

2 ISMS and GDPR – Veriscan ISM services (step #1)

2.1 ISMS situation for GDPR solutions

From an ISMS perspective there are two situations, both which Veriscan can support:

a) An ISMS is well established and may even be certified in the organization

b) An ISMS is not implemented

Depending on the situation the support is slightly different but the end results should be the same – "Use ISMS according to ISO/IEC 27001 to cover GDPR issues"

BUT it is important to state again, even if an ISMS (according to ISO/IEC 27001) is an advantage when addressing GDPR, there is no need to implement it fulfilling the requirement of the standard and getting into certification. The important savings to make is to take the advantages of the structured approach of an ISMS and use the basics. Veriscan ISM will address this and provide solutions depending on the situation and objectives of the client's organisation.

2.2 Adapting an existing ISMS for GDPR

The most straight forward support can be given if an ISMS is established. The support is mainly divided into the following:

- Scope and context – adding GDPR
- Policy and objectives – aligning with possible GDPR issues
- Organizational roles and responsibilities – adding/adjusting to the GDPR requirements concerning the roles in GDPR (data subject, controller, processor, third party, data protection officer)
- Assets - Adjusting assets and asset register
- Classification - Adjust classification and possibly add new impact assessments to cover the individual aspect as well as assess privacy data
- Risk - Review existing and possibly add risk assessments
- Controls – review selected controls and adjust (ISO/IEC 27001)
- Support implementation of additional or adjusted controls
- Any changes to the ISMS to cover GDPR as part of continual improvements

Which consultancy services of Veriscan ISM to be used, to address GDPR, in a situation with an existing ISMS, is typically based on the requirements and situation of the organization, such as:

- The time required using the existing ISMS process
- The size and complexity of the organization addressing GDPR
- The structure of the security organization
- The use of tools, existing and/or new

The service delivery will be handled as a project where the deliverables and project stages are defined together with the client. The project result will be an ISMS adaptation that will be structured in accordance with best practice.

2.3 Implementing an ISMS that comprises GDPR

The motives for implementing an ISMS in reflection of GDPR can be two folded:

a) The organization has decided to implement an ISMS regardless of GDPR, but naturally want GDPR to be part of the context and scope

b) The organization has decided to implement an ISMS to handle GDPR

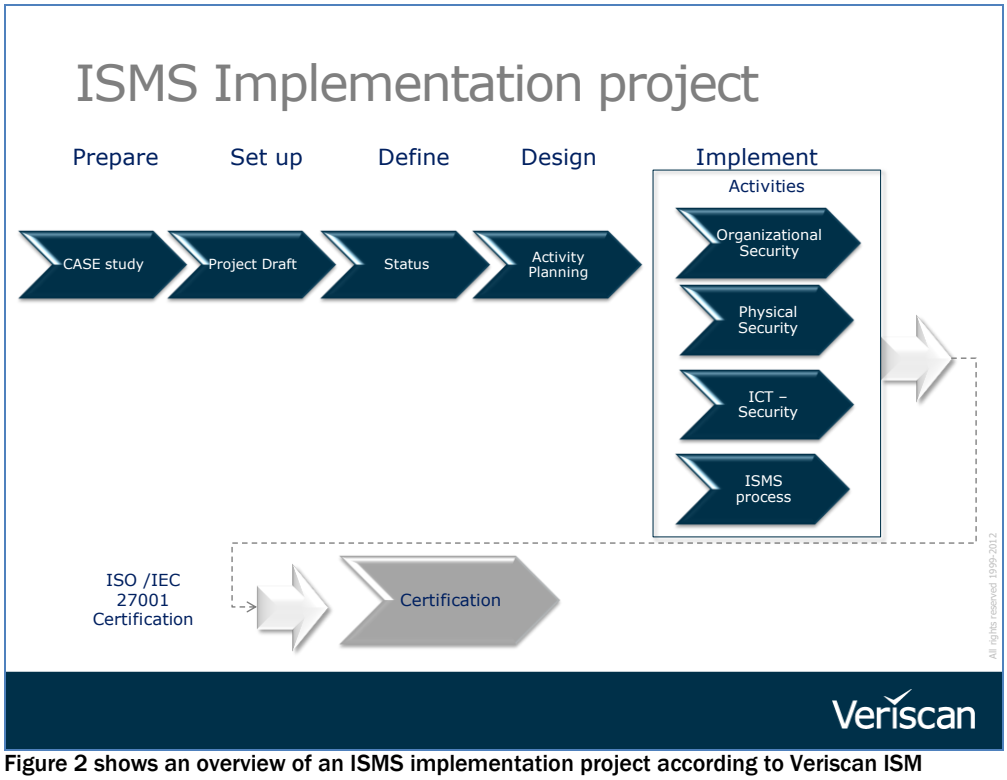


Figure 2 shows an overview of an ISMS implementation project according to Veriscan ISM

The Veriscan ISM service for implementation of ISO/IEC 27001 is done as a project. It has various phases based upon ISO/IEC 27003:2010, see figure above and details in Annex A – VERICAN ISM product sheet. When implementing an ISMS there are a number of issues to consider, e.g. external requirements and

which parties inside as well as outside the organization have an interest the ISMS. Adding GDPR to this context from start should be done regardless of the motives for implementing an ISMS. The implementation project, as such, may be designed differently depending on which of the two main motives that is applicable. There are typically other parameters that will influence the project much more than if GDPR is included from start or not.

The following requirements and situations of the organization will influence the design of an ISMS implementation project:

1) The time cycle of the Management System overall process
2) The size and complexity of the organization
3) The structure of the security organization
4) The use of tools
5) Objectives/business case/top management approval
6) Scope and boundaries
7) Time and resources
8) Internal organization as part of resources available for the project
9) Ambition on achieving certification

Regarding point 7, the time is of course very specific for GDPR, as there is a deadline of 25th of May 2018. Otherwise there is not much specific to be added except that GDPR has to be part of the ISMS and the GDPR requirements will be taken into account in the steps and activities when implementing the ISMS according to the Veriscan project model.

The consultancy services for Veriscan ISM for implementing an ISMS which is addressing GDPR, are based upon the points 1-9 described above.

The service delivery will be handled as a project where the deliverables and stages are defined together with the client. Naturally the ISMS implementation will be according to best practices applicable to the client organization.

3 Veriscan vIC tool (step #2)

3.1 The process for identification and classification of assets

The purpose of Veriscan vIC is to support the fulfilment of ISO/IEC 27001:2013 Annex A, clause 8, regarding the management of assets. The standard concerns information security assets, e.g. that they should be registered and classified and that owner ship should be specified etc. Veriscan vIC provides a flexible and efficient tool that enables complex relationships to be handled in an easy way and replace other inflexible solutions where the miscellaneous assets are stored in various registers or files.

Veriscan vIC is typically provided as right to use license. It is often used as a tool in Veriscan customer projects, e.g. a GDPR project.

There are three possible statuses of information assets when the use of Veriscan vIC is applicable:

1) No asset classification scheme is defined and no asset register is available;
2) A classification scheme exists but no registered assets available or incomplete register; or
3) A classification scheme exists and assets have been identified, evaluated and registered.

Furthermore, there are mainly three types of information assets that affect which approach to use in the process of identifying and classifying.

1) Information based on business processes and object used in these processes
2) Information resources based on IT services or systems
3) A combination of the above

Note: Non-digital information assets should also be included as assets but that is typically an extension of the approaches above.

Veriscan vIC has a work flow containing the following phases:

- Prepare – select the scope and assets within the scope as well as define the staff that can evaluate the impact
- Evaluate – go through each asset and classify the assets according to the scheme and rules determined by the organization (that is set up in the tool when configuring.)
- Finalize – review dependencies and determine final classification of the assets by the owner

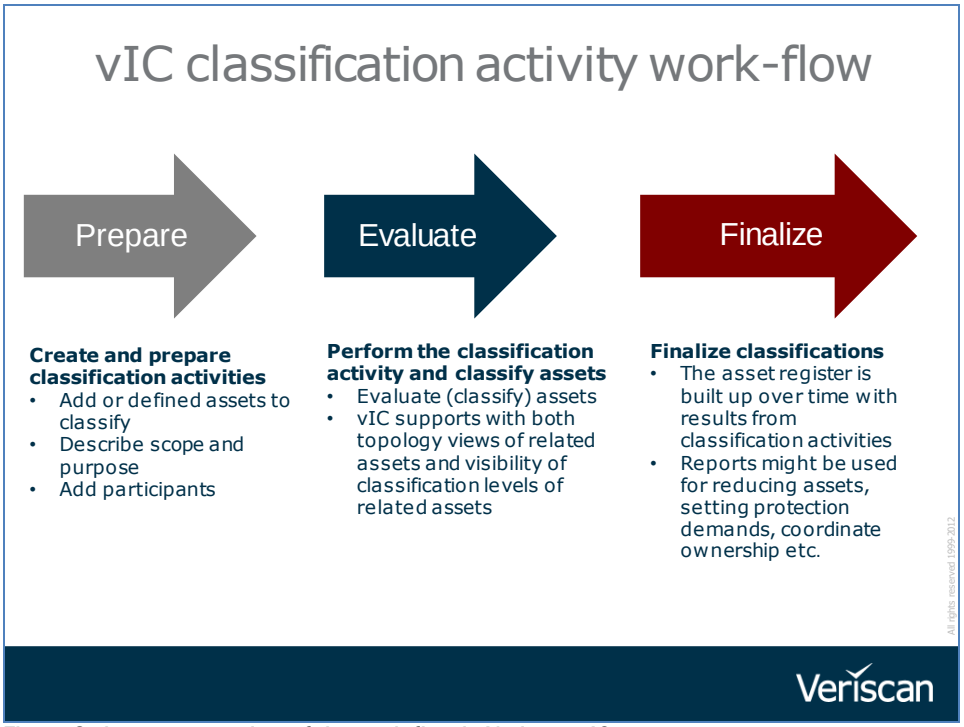


Figure 3 shows an overview of the work flow in Veriscan vIC

Veriscan vIC makes the work to identify and categorize assets efficient. The register of the assets are built up during the classification process described above. Note that also assets already identified in the register can be reassessed or assessed in a different context.

A relationship is created between various categories of assets to enable further classification and evaluate need of protection.

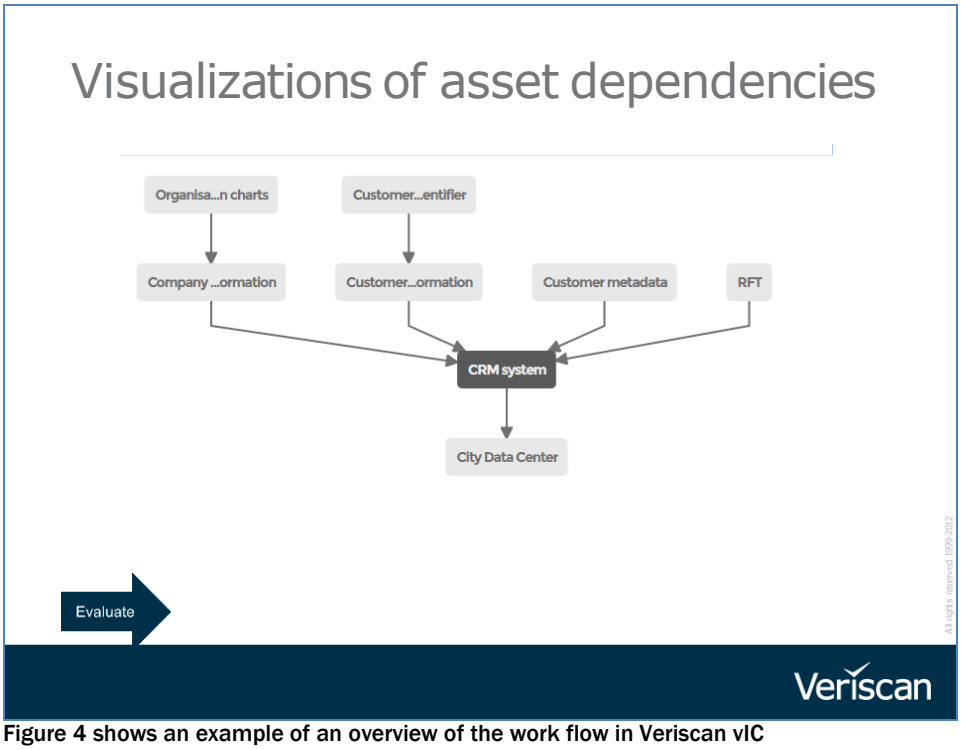


Figure 4 shows an example of an overview of the work flow in Veriscan vIC

3.2 Using Veriscan vIC for GDPR

Regardless of which of the three approaches described above, or combination of them, that is being used, the assets can be flagged to easily group specific assets of common concern. From a GDPR perspective assets concerning privacy and personal data can be flagged in a certain way and then selected to be used during the identification and impact analysis. This functionality in the Veriscan vIC makes it very practical and cost efficient.

The following steps describe the activities needed when an asset register is available.

- Configure the tool according to the information classification structure that is already decided
- Add all existing assets and their classification, categories etc.
- Determine what extra aspects are needed to cover the assessments regarding personal data according to GDPR
- Go through and flag assets that are or contain personal data according to GDPR.
- Review and select assets that are affected by GDPR and add impact aspects due to GDPR

If no assets register exists or a decision is made to start from scratch the steps are slightly different:

- Configure the tool according to what is needed including GDPR aspects
- Determine if personal data shall be identified directly or as a second step (first step means using flags and then go through them again as in the previous bullet list. In a smaller organization, where the amount of personal data, as assets, can be easily identified, it is possible to do it in one step. If there is a complex situation, the two-step approach is advisable.)
- Determine what assessments are needed and in which order the different scope of assets should be done
- Prepare the tool and carry out the assessments as decided
- Review the results and determine where impact is important and determine protection of personal data in accordance with GDPR requirements

Note: It is also a possible to tailor the Information assets scheme in vIC to include the specific requirements of GDPR which then will allow evaluation of compliance in a direct manner.

The result will in both cases be, that all important assets are identified and impact evaluated. Personal data related assets can be selected and special attention can be

given for the protection of these. The result will also serve as a basis for risk evaluation.

By using Veriscan vIC two main concerns in GDPR have been solved. The personal data is identified and the initial parts of an impact analysis have been conducted. It is easy to produce reports from the asset register which can be used to present the result.

4 Veriscan vRISK tool (step #3)

4.1 Supporting the risk process of an ISMS

The purpose of Veriscan vRISK is to perform risk management and as such also support the requirements of ISO/IEC 27001 clause 6.1. Veriscan vRISK addresses information security risks as well as the treatment of identified risks. Veriscan vRISK can also be used as a common tool for management of any type of risks. The tool supports the risk process required as stated in clause 8. It is a user friendly, flexible and cost-efficient tool. It is very easy to update the tool with new data that makes risk assessments efficient. Furthermore, the tool enables risks to be grouped and reported even from various risk entities and categories. It can replace other more inflexible solutions where the risk analysis and results are in different registers or files.

Veriscan vRISK is typically provided on a right to use license basis.

here are three situations when to use Veriscan vRISK:

1) Replacing existing solutions
2) As a new solution for ISMS specifically
3) As a new solution for multiple risk entities, in various organizational units, in addition to using it for information security risks

An important advantage of Veriscan vRISK is that it enables risks to be linked to multiple aspects. The result of using the tool can be summarized in many various ways and easy to read reports with text and graphs that can be produced to suit various target groups.

Veriscan vRISK can be easily configured at the time of the set-up of the tool. There are several options for configuration allowing the use of the tool to be optimized for the organization. Typical settings in the tool to be configured for the risk assessments are:

- Specification of categories of risk types, assets, control and objectives respectively
- Risk Matrix definition, e.g. level and size
- User privileges

Veriscan vRISK's work flow for a risk assessment consists of the following phases:

- Prepare – select the scope and staff that will carry out a risk assessment
- Define and evaluate – define risks and their risk level according to the scheme and rules determined by the organization (that is configured in the tool.)
- Treatment – determine risk owner and risk treatment options. If the risk should be reduced, activities and responsibilities are defined
- Follow up – When activities are completed the risk can be re-evaluated
- Reporting – producing reports with various levels of details and selections can be made in real time

4.2 About reports in Veriscan vRISK

The reporting can be done both for single risk assessments and aggregated for all or for selected assessments with several different groupings or selections. Reporting can also be done, comparing differences over time.

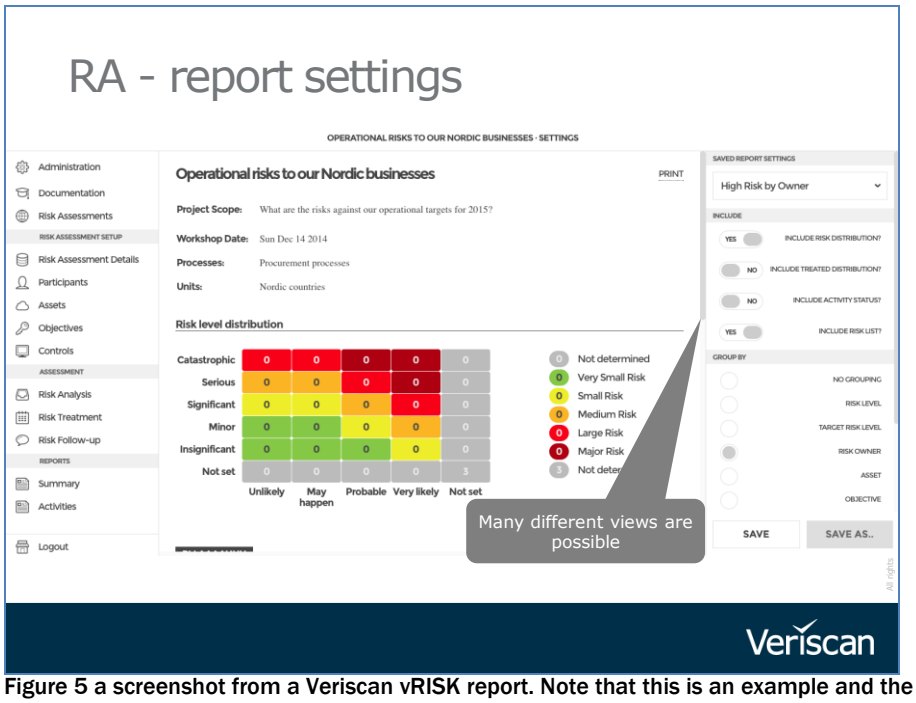


Figure 5 a screenshot from a Veriscan vRISK report. Note that this is an example and the actual possibilities and risk reports are depending on the individual set up of the tool.

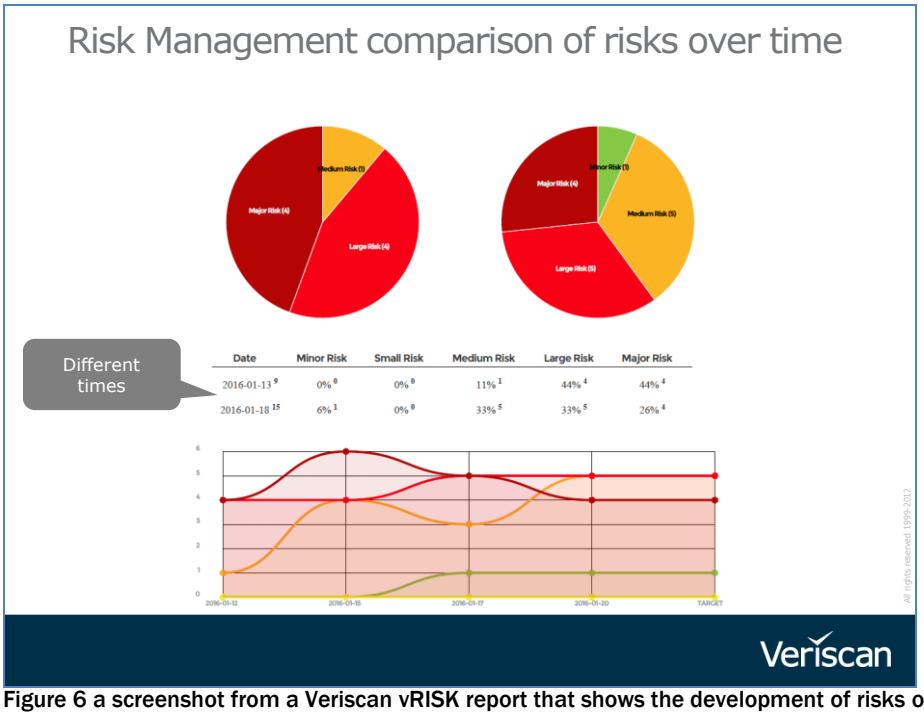


Figure 6 a screenshot from a Veriscan vRISK report that shows the development of risks over time (including several risk assessments). Note that this is an example. Reports can be tailored to the needs of an organization.

4.3 Using Veriscan vRISK for GDPR

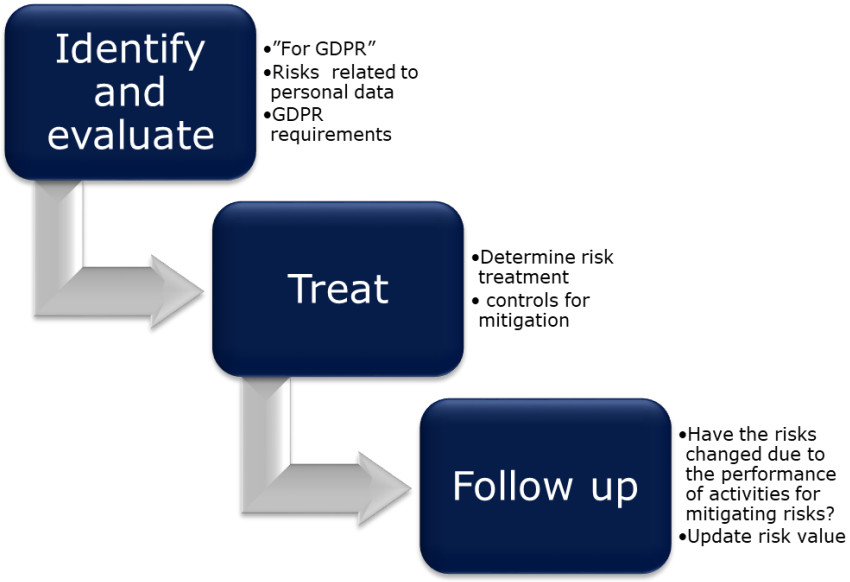


Figure 7 shows the principle work flow for a risk assessment in Veriscan vRISK and that GDPR issues come into the identification part as well as controls is needed.

Personal data protection risks must be evaluated to enable the proper protection of personal data. This evaluation is an important part of the mandatory data protection impact analysis. Veriscan vRISK can be used for addressing these risks and link them to the requirements in GDPR. If needed, the risk assessment can also be focused on personal data assets. Veriscan vRISK can compile reports, if needed, focused on risks related to GDPR. Furthermore, the result of using

Veriscan vRISK is an ideal basis to determine if specific controls for personal data protection are needed to reduce risk as well as adding controls that do not directly relate to information security, e.g. controls addressing consent and data minimization.

It is recommended that a specific GDPR control category is included in the Veriscan vRISK tool, which is defined in the configuration of the tool. Each identified risk, which applies to GDPR, is linked to the appropriate GDPR control in the GDPR control category. Veriscan vRISK enables defined activities, e.g. for risk reduction, to be linked to the specific GDPR risks. Using Veriscan vRISK, in the way described allow an efficient GDPR alignment. Veriscan vRISK supports production of reports targeting various groups of roles, e.g. top management. Veriscan vRISK also facilitates easy communication for distributing the responsibilities of risk management within the organization.

5 Veriscan Rating (step #4)

5.1 Performance measurements

The purpose of Veriscan Rating is to perform measurements of the level of security controls implemented and as such also support the performance evaluation in ISO/IEC 27001 clause 9 as well the controls in Annex A.

Veriscan Rating comprises of three parts:

- The Veriscan Rating method – stipulating how measurements are designed and creating a measurement program
- Veriscan vEAVER tool – based on the method to support the measurement process
- Veriscan Rating measurement programs – a complete set of measurements in a program based upon modules

Veriscan Rating is typically provided as a service but the method and the tool can be provided on a right to use license basis.

Performance measurements with Veriscan Rating is preferably repeated every 12-24 months, , to allow a consequent comparison of results over a longer period of time.

A typical Veriscan Rating project contains the following steps:

- Determine the scope of the measurement and select the measurement program
- Define the time when the measurement will be conducted
- Set up and conduct the measurements
- Reporting

The measurement programs are based upon various standard recommendations, regulations and best practices. The basic reference is ISO/IEC 27001 including the controls in Annex A and the guidance in ISO/IEC 27002. But one requirement of a control will typically result in a number of measurements to enable evaluating the performance.

In Veriscan Rating performance measurement programs, each measurement point is aimed at a certain measurement object rather than the regulation that it refers to. These measurement objects are numerous and a measurement program may include several hundred measurement points. There is a hierarchy of the measurement objects that enables structured reporting. There are also categories and areas that enable KPI presentation and evaluation.

The real benefit of Veriscan Rating comes when several measurements are done over a longer period of time. This allows the results of the performance measurements to be compared from one time to another.

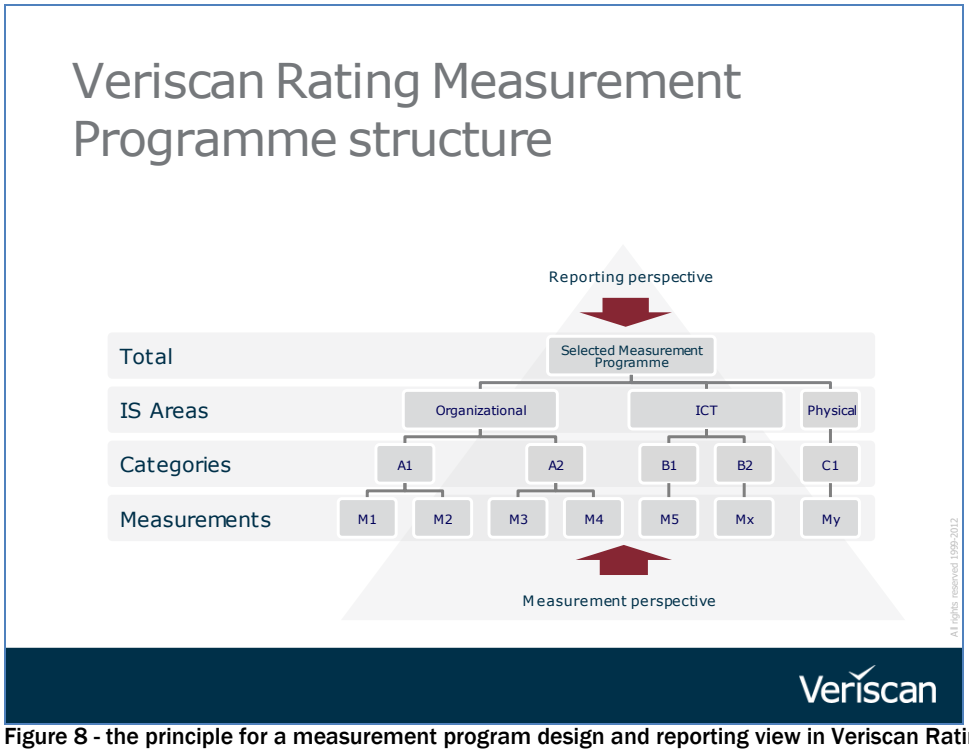


Figure 8 - the principle for a measurement program design and reporting view in Veriscan Rating

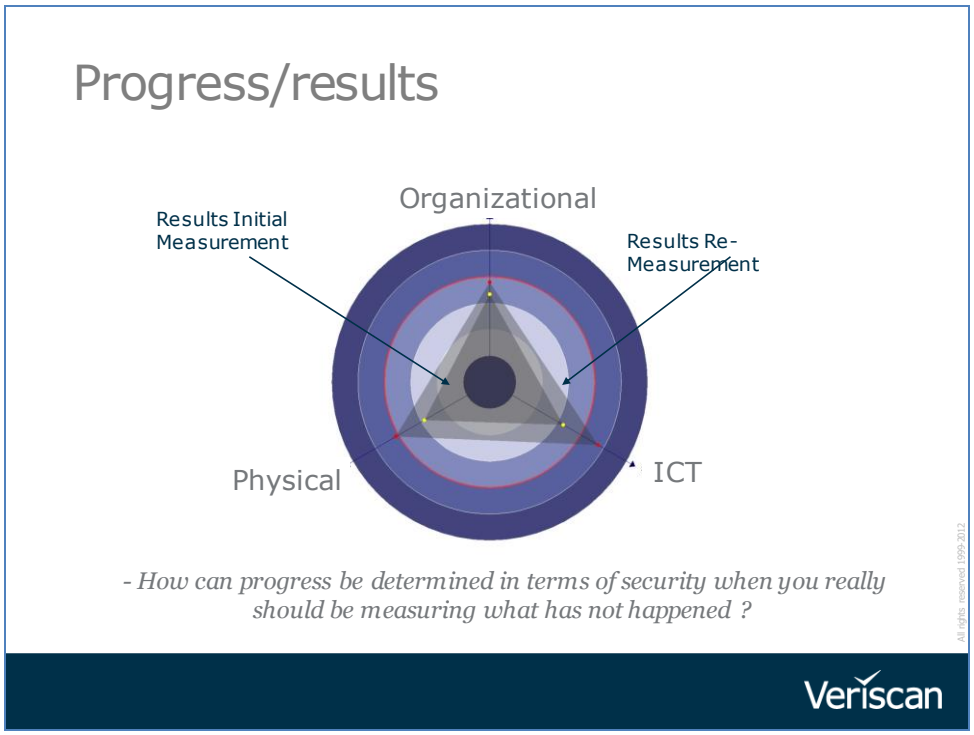


Figure 9 - a screenshot from a Veriscan Rating measurement report and the comparison with a second measurement

5.2 Using Veriscan Rating for GDPR

To measure an organization's information security management performance from a GDPR perspective is highly relevant. By adjusting and adding controls for data protection to Veriscan Rating it becomes an ideal tool for performance management. Veriscan Rating now has a specific module to cover the extra aspects/protection techniques and controls based upon ISO/IEC 29100 and ISO/IEC 29151 as well as on GDPR. This module can easily be added to the selected Veriscan Rating measurement program. The result of the performance measurement can be presented as part of the overall performance report as well as in a specific report for the added module.

Performance measurements using Veriscan Rating can provide strong evaluation indicators of GDPR compliance and be incorporated in the regular performance reporting to top management.