

# Risk Management Studio:

## An efficient and effective approach to risk assessment

By Knútur Birgir Otterstedt, M.Sc., Matthew Arnold, MBA  
& Svana Helen Bjornsdottir, Dipl.-Ing. / M.Sc.

January 9, 2012



---

### What is a risk assessment and what is the purpose of completing one?

---

Risk assessment is the overall process of risk analysis and risk evaluation of an organization, department, or business process, also known as a business entity. Risk assessment includes the evaluation of threats to an organization's assets, both tangible and intangible. It is an appraisal of the impact of threats on the assets in question, the vulnerability of assets towards the threats and the probability of the threats occurring. Risk assessment takes into consideration the scope and consequences of risk with respect to the nature of the information being processed. The objective of a risk assessment is to create conditions for the selection of mitigating controls and policies. A risk assessment should be completed and reviewed regularly in order to maintain best practices in regards to quality management systems (QMS).

The purpose of a risk assessment is to ensure the security and safety of an organization or specific entities within the organization. A risk assessment helps to:

- ◆ Create awareness of threats and risk to an organization, department or business process.
- ◆ Identify the assets that may be at risk.
- ◆ Determine if your current controls are sufficient for ensuring security, or if improvement to current controls or additional controls are needed.
- ◆ Identify the most significant threats and control measures.
- ◆ Prevent incidents or non-conformities.

The overall goal of the risk assessment process is to identify threats, minimize threats and reduce the level of risk to an organization's assets by

adding mitigating controls. By implementing such controls, an organization is creating a secure environment.

---

### How is a risk assessment completed?

---

A risk assessment should be completed by an individual or group within an organization with sound knowledge of the inner workings of the business

#### Risk Assessment Process

1. Identify the scope
2. Define the approach
3. Define the assets
4. Identify threats
5. Assess current controls
6. Establish new controls
7. Develop a risk treatment plan
8. Continually monitor risk

processes and management systems. Also, it cannot be stressed enough how important it is to have top management involved, understand a risk assessment is being completed and have its "buy in" giving access to the required resources. Staff members who are an organization's experts in a specific area and are well versed in the in specific operations should be consulted when completing a risk assessment. If completing a risk assessment for certification by a standards organization, it is beneficial to understand the standard, the requirements and the overall objective of the standard.

#### The Risk Assessment Process

- ◆ The risk assessment process begins by identifying the scope of the assessment. Will you be assessing your organization as a whole, or a single department? The scope can vary based on your objectives.
- ◆ Next, define the risk assessment approach. Will you utilize a quantitative or qualitative approach, or perhaps a combination of the two? Will you employ the services of a third party to assist in the process?

- ◆ Define the assets within the scope of your assessment and the associated significance of the assets to your organization. Assets are tangible or intangible economic resources which can be owned or used to produce value.
- ◆ Identify relevant threats towards the assets, identification of vulnerabilities of the asset towards each threat, impact of threat and the probability of a threat becoming a reality.
- ◆ Identify and determine if current controls are sufficient enough to mitigate risk.
- ◆ Establish new actions and controls that need to be implemented in order to eliminate or control risk.
- ◆ A risk treatment plan should be developed and the treatment options should be chosen based on results of the risk assessment, cost of implementation and expected benefits of these options.
- ◆ Upon completion, continuously monitor and evaluate to assure risk is controlled.
- ◆ It is important that the process used, such as the criteria for measuring the values associated with the risk is consistent and repeatable each time an assessment is completed.

3. Documents are easily shared and transferable between computers
4. Customizable format

**One time risk assessment for smaller organizations:** When small organizations with limited operations need to complete a single risk assessment, it may prove beneficial to complete the risk assessment utilizing a spreadsheet program. However, if the assessment needs to be repeated, or components of the assessment begin to become numerous, the task may soon become tedious.

**No purchase if a spreadsheet program is already owned by an organization:** Most organizations have already purchased a spreadsheet program or utilize open source spreadsheet programs negating the need to purchase a spreadsheet program.

**Documents are easily shared and transferable between computers:** When organizations have an enterprise version of a spreadsheet program, risk assessments can easily be emailed, or placed on collaboration software to allow for sharing throughout the organization.

**Customizable format:** Risk managers using spreadsheet programs have the option of customizing all aspects of the risk assessment, from calculations to aesthetics.

- Limitations of spreadsheet programs**  
The limitations of spreadsheet programs can increase the cost, time and resources needed to complete risk assessment projects. These limitations include:
1. Sharing and unprotected documents
  2. Calculation creation
  3. Formula errors, human errors and cell linking
  4. Starting with a blank document
  5. Repeatability
  6. Multiple worksheets/workbooks

**Sharing and Unprotected document:** When sharing the risk assessment as a document, you run the risk of edits and changes being made without the document owner's consent. This could lead to an unapproved version making its way to publication, without record of when the changes were made. Further, unauthorized users

---

## The use of spreadsheet programs for risk assessment

---

Spreadsheet programs are an essential aspect of businesses and are utilized for a wide variety of tasks. The adaptability of spreadsheet programs lead to their use without consideration for other solutions. This is often the case when these programs are utilized for risk assessments. Spreadsheet programs offer features and attributes that are beneficial for risk managers, but do come with limitations.

*The risk assessment process can be a complicated task without the right tools in place.*

### Positive attributes of spreadsheet programs

The positive attributes and appropriate times for the use of spreadsheet programs include:

1. One time risk assessment for smaller organizations
2. No purchase if a spreadsheet program is already owned by the organization

may gain access to the documents if proper precautions are not taken when sharing the documents on local servers or via email.

**Calculation creation:** When utilizing spreadsheets for a risk assessment, users will need to create or research risk calculations to implement. This can be a daunting task and be very time consuming. Further, when implementing the calculations, the risk of utilizing formulas that are not consistent throughout the scope of the assessment increases.

**Formula errors, human errors and cell linking:** Whether completing financial budgets or risk assessments, when utilizing spreadsheets the danger of formula errors is always present. Simple mistakes such as putting a decimal in the wrong spot or a link with an incorrect cell can lead to an erroneous report.

**Starting with a blank document:** When utilizing spreadsheet programs, users usually need to create all aspects of the risk assessment. From naming tabs, to formatting columns, this can be a time consuming task.

**Reports and formatting:** Risk managers are required to create their own reports based of the data contained within the spreadsheet programs. This can cause issues with carrying over the correct, relevant information needed for auditors; formatting issues can occur and can be time consuming to create the documents in an easy to read and understandable format.

**Repeatability:** Risk assessments are generally completed annually for auditing purposes (certification renewal) and for continuous improvement. Spreadsheet program risk assessments may not be setup to be easily repeatable.

If the risk manager who creates the risk assessment leaves an organization, the process and methodology used may not be clear without proper documentation. If this documentation is not included with the assessment, a new assessment may need to be created.

**Multiple worksheets/workbooks:** The risk assessment process and documentation can

quickly become overwhelming if contained in multiple worksheets and workbooks.

---

## **RM Studio, risk management software that simplifies the risk assessment process**

---

RM Studio is full-featured, customizable and dynamic risk management software that increases efficiency. Developed by ISMS experts with the goal to simplify risk management, RM Studio guides users through the complex process of risk assessment, risk treatment and risk management.

*“The time-saving achieved with the incorporation of expert-knowledge within the tool is not to be under-estimated.” - StatPro*

RM Studio is modular software that allows users to embed international standards and deploy risk management modules, including a risk assessment module and a business continuity module.

### **RM Studio’s Key Benefits for Risk Assessment Process**

RM Studio offers an all-in-one solution that assists in managing and addressing risk, controls, and risk treatment objectives in an intuitive, simple, and easily managed way. RM Studio provides an overview of the entire risk assessment process, allowing users to quickly see the base, current and future security risk status. The key benefits of using RM Studio for risk assessments are:

1. Integrated asset categories and threat library
2. Embedded standard option
3. Easily repeatable processes and embedded evaluation templates
4. Benchmark risk calculations
5. Integrated implementation guide
6. Linked gap analysis and risk treatment plan
7. Integrated Reporting

#### **Integrated asset categories and threat library:**

RM Studio comes with a predefined asset category library and a predefined threat library which are connected, helping users to identify important and derivative threats. Assets are easily categorized with the comprehensive asset category library, removing the guesswork from the risk assessment process. Users are also able to

create their own asset categories to meet specific organizational needs.

The embedded threat library automatically connects the associated threats to the asset categories. Threats can also be added and removed by the user to develop an assessment that is suitable for the organization.

RM Studio's functionality allows for the relationship between assets and threats to be viewed with the click of a button, allowing users to quickly see the threats associated with a single asset or vice-versa.

**Embedded standards option:** International accredited standards, including, but not limited to, International Organization for Standardization (ISO) standards, Payment Card Industry Data Security Standards, and the World Lottery Association Security Control Standard can be embedded and easily deployed. Other standards specific to organizations can be inputted by the user or the RM Studio team meeting the demands of an ever changing market.

**Easily repeatable processes and embedded evaluation templates:** RM Studio's evaluation templates are based on industry best practices and are ready to be deployed at the click of a button, ergo simplifying the risk assessment process. Users can also implement evaluation criteria based on current needs, allowing for dynamic responses to an ever changing market.

**Benchmark risk calculations:** The risk calculations which RM Studio utilizes were developed by ISMS experts. The coverage of risk calculation is scalable by the user with little effort when necessary.

RM Studio utilizes built-in asset evaluation criteria and threat evaluation criteria to automatically calculate the risk value, simplifying the process for users. Further, users can also implement their own evaluation criteria for assets and threats. Evaluations can be based on internal processes, international standards, or other evaluation criteria, allowing for evaluation based on organization specific needs.

**Integrated implementation guide:** RM Studio, when embedded with standards, includes the

implementation guide for said standards. User can utilize the integrated implementation guide to assist in mitigating risk and putting controls in place, as well as for designing organizational policy. Users can also outline their own implementation guides for existing or user defined standards.

**Linked gap analysis and risk treatment plan:**

Upon completion of the risk assessment process, RM Studio connects the next steps of the process, gap analysis and risk treatment planning. Users can utilize the Gap Analysis feature of RM Studio for a quick and simplified compliance check. The Gap Analysis feature guides users through the implementation of controls towards an appropriate risk appetite. RM Studio also simplifies the tracking of implemented controls and responsible parties for carrying out the required actions. The Gap Analysis feature, when used with embedded standards, also provides an in-depth implementation guide based on the various standards.

**RM Studio is proven to:**

- ✓ Simplify the risk management process
- ✓ Reduce complexity and costs
- ✓ Assist in the certification process
- ✓ Identify informational assets & evaluate threats
- ✓ Ensure traceability
- ✓ Reduce consultancy cost

RM Studio further simplifies the overall risk assessment process with its integrated Risk Treatment feature. The Risk Treatment feature automatically merges the risk assessment and gap analysis into one

centralized repository, where current and future security risk are automatically calculated and compared to the base security risk calculated during the risk assessment. Users are then guided through the process of determining the appropriate risk treatment decision, which are; avoid risk, reduce risk, accept risk, or transfer risk.

**Integrated reporting and exporting options:** RM Studio comes equipped with 11 preformatted reports, available at the click of the button, such as a detailed Risk Assessment Report, Statement of Applicability, Gap Analysis Results, and an Executive Summary. All data within RM Studio can easily be exported to Excel or PDF at the click of a button.

---

## Testimonials from RM Studio Users

---

**StatPro:** “StatPro chose RM Studio over other similar products because its ease of use when setting up an Information Asset Register and conducting a Risk Assessment and the scope and depth of reporting at each stage of the risk-management process.”

“The time-saving achieved with the incorporation of expert-knowledge within the tool is not to be under-estimated. Relevant threats are pre-mapped to different information asset categories, allowing the user to focus on organization-specific asset-value and threat-assessment data. RM Studio's flexibility enables the relevant threats to be customized.”

**Síminn:** “Síminn has been using RM Studio since the beginning of 2010. We have found RM Studio indispensable in our risk management work. The software helps to simplify our environment and keep track of information risk.”

**Cooperativa Financiera de Antioquia:** “Identifying types of assets, threats and controls is a never ending task. To compile all that information in an Excel spreadsheet is even more complicated. The implementation of RM Studio has facilitated the realization of risk analysis and most importantly, we have reduced working time. RM Studio is a very intuitive and easy to use tool.”

**Entraction:** “RM Studio was easy to install, simple to navigate and extremely flexible. RM Studio certainly saved us countless hours of work.”

**Kreditkort:** “RM Studio is a very powerful tool for performing such complex task as the identification of information assets and risk assessments. RM Studio managed projects well and led the company through the preparation of a risk assessment. The software provided a comprehensive overview of the company's security issues and performed the tasks efficiently. RM Studio returns clear results in an accessible format, making it easier for both the company and regulators to see the status of the

company in this area, as well as integrating well with the company's internal auditing system”

**TM Software:** “RM Studio has proved successful for TM Software in preparing risk assessments, has saved time when alterations have been made to the risk assessment, and is necessary to maintain our ISO certification. All results of the risk assessment are in one location and are easy to access. The first risk assessment for TM Software was contained in a large number of documents and was time consuming to use – now we need only RM Studio. All assets of importance to the operation of companies can be stored in RM Studio; it is easy to access list of assets and parties responsible for assets, as well as the controls that apply.”

**Landsvirkjun:** “The Landsvirkjun risk assessment was prepared using RM Studio, which facilitated the assessment process and saved substantial time.”

---

## Summary

---

The risk assessment process can be a complicated task without the right tools in place. Organizations must actively identify and mitigate risk before they occur to ensure reliable service and maintain the organization's reputation. Most organizations unfortunately utilize manual methodologies through spreadsheet programs to the complete risk assessment process. While spreadsheet programs offer their own advantages, the limitations far outweigh the benefits. By not using an automated, centralized tool to complete risk assessments, organizations fail to connect and properly assess the risk variables at hand and distinguish the organizations overarching risk position.

RM Studio users have found that the solution simplifies the risk assessment process, enabling them to proactively identify the threats to the organization's assets, evaluate the impact, probability, and vulnerability of those threats, correlate them to controls, and track the results in a centralized solution. RM Studio is suitable for all organizations within all industries looking to automate, streamline and simplify the risk management process.

---

## About the authors

---



Knútur Birgir Otterstedt serves as a quality and security manager at Stiki. Mr. Otterstedt is responsible for product development and testing, conducting client and internal audits, measuring security and quality controls, and information security and quality assurance consultancy for clients. He is also accountable for the implementation of quality management systems and information security management systems based on international standards, e.g. ISO 9001, ISO 27001, and ISO 20000. Mr. Otterstedt graduated with a M.Sc. degree in industrial engineering from the University of Iceland.



As the Key Account Manager for RM Studio, Matthew Arnold is responsible for global marketing, sales and account management for RM Studio. He is also responsible for business development and global strategy planning. Mr. Arnold has more than five years of account management experience within the management consulting, insurance and information security industries, with a focus on international client bases and global markets. Mr. Arnold holds a MBA in International Business from The University of Tampa, an AACSB International accredited university.



Svana Helen Björnsdóttir is the Founder, board member and Chief Executive Officer of Stiki. Ms. Björnsdóttir has many years of experience in project management and consultancy regarding various aspects of information security, risk assessment and risk management. With extensive knowledge of international standards such as ISO 9001 and ISO 27001, she has pioneered their use in Iceland. Ms. Björnsdóttir holds a *Diplom-Ingenieur*/M.Sc. degree in electrical engineering from the Technical University of Darmstadt in Germany.

RM Studio is developed by Stiki, a leading provider of information security management solutions & among the first to achieve ISO/IEC 27001 certification. Stiki specializes in consulting software solutions.