

Information Risk Management Framework

Information Security



|  |  |  |
| --- | --- | --- |
|  |  | |
| Risk Management Framework | |  |
| Nummer | [Nummer] | |
| Erlassen am | 15.12.2023 | |
| Durch | Chief Information Security Officer | |
| Inkrafttreten | 15.12.2023 | |
| Geltungsbereich | SÜDVERS Holding GmbH & Co. KG und deren Tochtergesellschaften mit Mehrheitsbeteiligung, sowie die SÜDVERS International GmbH | |
| Thema | Risk Management | |
| Verantwortliche Funktion | Information Security | |
| Verantwortliche Person | Dirk Franken | |
| Übergeordnete Vorschrift | Information Security Policy | |
| Ersetzt | n/a | |
| Mitgeltende Dokumente |  | |
| Gültigkeit | Bis auf Widerruf | |
| Letzte Überprüfung | 14.07.2025 | |
| Nächste Überprüfung | 07.01.2026 | |
| Publikation | SÜDVERS Intranet | |
| Klassifizierung | Intern | |
| Archiv | Dokumentenverwaltungssystem | |
| Ordnungssystem | [Ordnungssystem] | |
| Sprachen | Englisch | |
| Formate | Online | |
| Bemerkungen |  | |

Inhaltsverzeichnis

[1 Information Risk Assessment Framework 4](#_Toc152589315)

[1.1 Management Approach 4](#_Toc152589316)

[1.1.1 Principle 4](#_Toc152589317)

[1.1.2 Objective 4](#_Toc152589318)

[1.1.3 Controls 4](#_Toc152589319)

[1.2 Information Risk Assessment Methodology 6](#_Toc152589320)

[1.2.1 Principle 6](#_Toc152589321)

[1.2.2 Objective 6](#_Toc152589322)

[1.2.3 Controls 6](#_Toc152589323)

[1.2.4 About IRAM2 6](#_Toc152589324)

[2 Information Risk Assessment Process 7](#_Toc152589325)

[2.1 Scoping 8](#_Toc152589326)

[2.2 Business Impact Assessment 8](#_Toc152589327)

[2.2.1 Business Impact Reference Table 8](#_Toc152589328)

[2.3 General Accepted Risk Levels 9](#_Toc152589329)

[2.4 Threat Profiling 9](#_Toc152589330)

[2.5 Vulnerability Assessment 10](#_Toc152589331)

[2.6 Risk Evaluation 10](#_Toc152589332)

[2.7 Risk Treatment 10](#_Toc152589333)

# Information Risk Assessment Framework

## Management Approach

### Principle

Information risk assessments must be performed for target environments (such as critical business environments and applications (including those under development); and supporting technical infrastructure).

### Objective

To enable individuals who are responsible for target environments to identify key information risks, evaluate them and determine the treatment required to keep those risks within acceptable limits.

### Controls

SÜDVERS will follow ISF IRAM2 for managing information risks.

Based on the selected ISF IRAM2 approach standards/procedures cover the:

* types of target environment that need to be assessed for Information risks (such as critical business environments, processes and applications; industrial control systems and supporting systems/networks)
* circumstances in which Information risk assessments should be performed (such as as part of systems development, following major business changes or where business services might be outsourced)
* individuals who need to be involved at each phase of Information risk assessments, and their specific responsibilities
* methods of managing and responding to the results of Information risk assessments
* mechanisms to take account of the results of security-related issues in operational risk assessments, security reviews or audits

Based on the selected ISF IRAM2 approach Information risk assessments should be performed for a range of critical target environments, including:

* information assets
* business applications
* systems and networks that support business processes and applications (including storage systems, databases, firewalls and authentication servers)
* operating environments (such data centers)

Decision-makers including executive management, heads of business units/departments and system owners, should be aware of the need to carry out Information risk assessments for critical target environments within SÜDVERS.

Information risk assessments have to be performed when:

* undertaking major business changes (such as new business ventures; business transformation programs; and mergers and acquisitions)
* introducing significant new technologies (such as the Internet of Things (IoT))
* there is an increase in the frequency and impact of serious cyber-attacks in the industry sector in which SÜDVERS operates

Business applications and supporting environments should be subject to an Information risk assessment:

* at different stages in their development, particularly during the early stages of the development lifecycle
* prior to significant changes (such as permitting access from additional jurisdictions, processing government information or migrating to web-based technology)
* when considering if they should be outsourced to an external party, such as a managed service provider (such as through the cloud)

Based on the selected ISF IRAM2 approach Information risk assessments involve:

* business owners (including information owners and owners of business environments, processes or applications)
* IT specialists, service managers and technical architects
* senior representatives from business support functions,
* information security specialists

Results from Information risk assessments conducted across SÜDVERS must be:

* reported to key stakeholders, including business owners and executive management (or equivalent)
* used to help determine programs of work in information security
* used to demonstrate adherence to internal policies and compliance with external standards and legal/regulatory requirements

## Information Risk Assessment Methodology

### Principle

Information risk assessments must be undertaken using systematic and structured methodologies.

### Objective

To make Information risk assessments effective, easy to conduct and consistent throughout SÜDVERS and to produce a clear picture of key information risks.

### Controls

SÜDVERS will apply ISF IRAM2 as its Information risk assessment methodology.

### About IRAM2

The ISF IRAM2 is a practical methodology that helps businesses to identify, analyse and treat information risk throughout SÜDVERS. In the updated version, “react and prepare” have been incorporated into the supporting information used during the threat profiling phase, including the common threat list and the threat event catalogue.

Also, on the vulnerability front, the previous IRAM control library, consisting of 29 controls, has been replaced with a more comprehensive set of 167 controls based on ISF “The Standard of Good Practice for Information Security”. The approach for determining control strength also now includes the extent of ‘relevance’ and ‘implementation’ of environmental controls. This enhanced approach is supported with the introduction of control relevance tables to provide objectivity and repeatability.

Its supporting tool, the IRAM Assistant, was previously a single, Excel-based supporting tool. It has now been split into four integrated modules collectively referred to as the IRAM2 Assistants. Each module supports one or more phases of the methodology. The IRAM2 Assistants automate parts of the methodology that would otherwise require a greater amount of manual effort and offer in-depth analysis to enhance business decision making. They also deliver specific templates that can be applied for enterprise-wide information risk assessments and use report templates to convey the key risks to stakeholders.

IRAM2 provides SÜDVERS with the ability to tailor their threat tables to reflect the SÜDVERS overall risk appetite. IRAM2 works by evaluating and assessing a variety of information risk factors that comprise each information risk equation. Once defined at SÜDVERS level, risk appetite can be communicated and presented differently throughout an organization. If an organization does not have a defined risk appetite, the decisions regarding the treatment for each risk will have to be made by the key stakeholders on a risk-by-risk basis. The practitioner should make the key stakeholders aware that the lack of a defined risk appetite could result in inconsistent decisions regarding the amount of risk the SÜDVERS accepts.

# Information Risk Assessment Process

The Information risk assessment process as implemented by SÜDVERS is aligned with ISO 31000 and looks schematically as follows

Ein Bild, das Text, Screenshot, Diagramm, Reihe enthält.

Automatisch generierte Beschreibung

On a more practical / technical implementation, SÜDVERS has decided to implement the process as defined by ISF IRAM2.

IRAM2 is set out in six phases. Each phase details the steps and key activities required to achieve the phase objectives, as well as identifying the key information risk factors and outputs.

At high level, the process is structured as follows:

Ein Bild, das Text, Screenshot, Schrift, Diagramm enthält.

Automatisch generierte Beschreibung

## Scoping

This phase of the risk assessment process is used to provide an integrated view of risk from the business service layer down to the technology infrastructure.

As SÜDVERS follows ISF IRAM2 in its most up-to-date version, more details about this phase can be found in the related ISF IRAM2 report and the related practitioners’ guides.

## Business Impact Assessment

This phase of the risk assessment process is used to determine the potential business impact (on a company level) should information assets or systems have their confidentiality, integrity or availability compromised.

As SÜDVERS follows ISF IRAM2 in its most up-to-date version, more details about this phase can be found in the related ISF IRAM2 report and the related practitioners’ guides.

### Business Impact Reference Table

A business impact reference table (BIRT) contains a categorised list of the most common types of business impact that an organisation could suffer as a result of the loss of one (or more) information attributes, along with guidance to determine the potential impact rating of each type.

To address this, a BIRT needs to be defined specifically for each organisation to best reflect the relevant impact categories, and to help determine the impact rating within each category, corresponding to each level of organisational impact (negligible, low, moderate and high).

For the purpose of SÜDVERS business impact assessments SÜDVERS defines the business impact reference table as follows:

Ein Bild, das Text, Screenshot, Zahl, Schrift enthält.

Automatisch generierte Beschreibung

SÜDVERS defines a system to be critical as of the DORA regulation and the related RTS in case of a business impact category rating of “high”.

In case that SÜDVERS is asked to perform business impact assessments on behalf of a customer, the customer’s BIRT has to be used.

## General Accepted Risk Levels

The SÜDVERS board of directors have, based on the BIRT as shown above, defined the followed levels for generally accepted risks for SÜDVERS:

Ein Bild, das Text, Reihe, Software, Screenshot enthält.

Automatisch generierte Beschreibung

## Threat Profiling

This phase of the risk assessment process is used to identify and profile key threats across different groups by determining associated threat events.

As SÜDVERS follows ISF IRAM2 in its most up-to-date version, more details about this phase can be found in the related ISF IRAM2 report and the related practitioners’ guides.

## Vulnerability Assessment

This phase of the risk assessment process is used to examine the extent of relevance and implementation of key controls that will help to determine control strength.

As SÜDVERS follows ISF IRAM2 in its most up-to-date version, more details about this phase can be found in the related ISF IRAM2 report and the related practitioners’ guides.

## Risk Evaluation

This phase of the risk assessment process is used to map the likelihood of successful threat events to the most appropriate business impact scenario and to link this into the wider SÜDVERS risk framework.

As SÜDVERS follows ISF IRAM2 in its most up-to-date version, more details about this phase can be found in the related ISF IRAM2 report and the related practitioners’ guides.

## Risk Treatment

This phase of the risk assessment process is used to explore different approaches to treating information risk (such as mitigation (reduction), avoidance, transference and acceptance (retention)).

Ein Bild, das Text, Screenshot, Diagramm, Schrift enthält.

Automatisch generierte Beschreibung

As SÜDVERS follows ISF IRAM2 in its most up-to-date version, more details about this phase can be found in the related ISF IRAM2 report and the related practitioners’ guides.