**C:\Users\juan\AppData\Local\Microsoft\Windows\INetCache\Content.Word\Logo_caseslu.emf**

**${DOCUMENT}**

**${COMPANY}**

**Informationssicherheit -**

**MONARC**

**Allgemeine Hinweise**

Version : ${VERSION}

Dokumentstatus: ${STATE}

Klassifizierung: ${CLASSIFICATION}

Unternehmen: ${COMPANY}

Name des Dokuments: ${DOCUMENT}

Datum: ${DATE}

Sicherheitsberater: ${SMILE}

Vertreter des Kunden: ${CLIENT}

**Zusammenfassung**

${SUMMARY\_EVAL\_RISK}

**Aktuelle Risikokarte**

${CURRENT\_RISK\_MAP}

**Ziel Risikokarte**

${TARGET\_RISK\_MAP}

Inhaltsübersicht

[1 Einleitung 4](#_Toc9335013)

[1.2 Zweck des Dokuments 4](#_Toc9335014)

[1.3 Quellenangaben 4](#_Toc9335015)

[1.4 Akronyme/Begriffe 4](#_Toc9335016)

[1.5 Beschreibung der “Méthode Optimisée d’Analyse des Risques CASES” (MONARC) 5](#_Toc9335017)

[2 Bestimmung des Kontextes 8](#_Toc9335018)

[2.1 Beschreibung des Kontextes 8](#_Toc9335019)

[2.2 Festlegung der Kriterien für die Risikobewertung 8](#_Toc9335020)

[2.2.1 Skala Auswirkungen 8](#_Toc9335021)

[2.2.2 Skala Bedrohungen 8](#_Toc9335022)

[2.2.3 Skala Sicherheitslücken 8](#_Toc9335023)

[2.2.4 Tabelle der Risiken und Risikoakzeptanzschwellen 9](#_Toc9335024)

[2.3 Bewertung der Tendenzen und der Bedrohungen 10](#_Toc9335025)

[3 Modellierung des Kontextes 11](#_Toc9335026)

[3.1 Identifizierung der Assets 11](#_Toc9335027)

[3.2 Identifizierung der Sicherheitslücken 11](#_Toc9335028)

[3.3 Einschätzung der Konsequenzen 11](#_Toc9335029)

[4 Risikobewertung und Risikobehandlung 12](#_Toc9335030)

[4.1 Zusammenfassung der Risikobewertung 12](#_Toc9335031)

[4.2 Risikobehandlung 13](#_Toc9335032)

[4.2.1 Risiken der Informationen 13](#_Toc9335033)

[4.2.2 Operative Risiken 13](#_Toc9335034)

[Anhang A: Interview und Informationsbeschaffung 14](#_Toc9335035)

[Anhang B: Bewertung der Tendenzen 15](#_Toc9335036)

[Anhang C: Bewertung der Bedrohungen 16](#_Toc9335037)

[Anhang D: Hinweise und Bemerkungen des Beraters 17](#_Toc9335038)

[Risiken der Informationen 17](#_Toc9335039)

[Operative Risiken 18](#_Toc9335040)

# Einleitung

* 1. **Kontext der Risikoanalyse**

${CONTEXT\_ANA\_RISK}

## Zweck des Dokuments

Dieses Dokument enthält eine Zusammenfassung der Methodik und die Ergebnisse der mit MONARC in der Kundenumgebung durchgeführten Risikoanalyse. MONARC orientiert sich an der internationalen Norm ISO 27005:2011.

Die Ergebnisse sollen helfen, größere Risiken zu erkennen und das bestehende Sicherheitsniveau zu verstehen, und geben Empfehlungen für die Ergreifung von Sicherheitsmaßnahmen. Den Parteien ist bekannt, dass die Empfehlungen weder ausschließlich noch erschöpfend sind.

Die Liste der festgestellten Risiken basiert auf den vom Kunden und/oder seinen Vertretern bereitgestellten Informationen, ohne dass dafür Nachweise erbracht werden mussten. Die sich aus dieser Bewertung ergebende Analyse begründet keine Haftung von SMILE GIE für Auslassungen oder Fehlern von Dritten oder nicht.

## Quellenangaben

1. ISO/IEC 27005 (2011), Informationssicherheits-Risikomanagement.
2. <http://www.iso.org/iso/en/catalogue_detail?csnumber=56742>. Die Norm ISO 27005 erklärt im Detail, wie Risikobewertung und Risikobehandlung im Bereich der Informationssicherheit erfolgen sollen.

## Akronyme/Begriffe

**Asset:** Jedes Element, das für die Einrichtung einen Wert darstellt.

**Vertraulichkeit:** Eigenschaft einer Information, dass diese für unbefugte Personen, Stellen oder Prozesse nicht verfügbar ist und nicht offengelegt wird.

**Verfügbarkeit:** Eigenschaft einer Sache, die auf Anfrage einer befugten Stelle zugänglich und nutzbar ist.

**Integrität:** Eigenschaft, die Richtigkeit und Vollständigkeit eines Assets zu bewahren.

**MONARC:** Méthode Optimisée d’Analyse des Risques CASES – Methode für optimierte Risikoanalysen.

## Beschreibung der “Méthode Optimisée d’Analyse des Risques CASES” (MONARC)

Die Risikoanalysemethode MONARC besteht aus vier Phasen:



Konkret bedeutet das:



MONARC vereinfacht das Risikomanagement, indem eine Lösung für Risikomanagement und Steuerung der Informationssicherheit basierend auf den neuesten Erkenntnissen des Fachgebiets bereitgestellt wird. Mithilfe dieser Methode ist innerhalb kurzer Zeit eine Analyse auf Grundlage vorhandener und personalisierbarer Modelle gemäß den Vorgaben der internationalen Norm ISO/IEC 27005:2011 möglich.

MONARC stützt sich auf eine Bibliothek mit Risikomodellen, die Objekte bereitstellen, welche sich aus Risikoszenarien für Assets oder Gruppen von Assets zusammensetzen. Dieser Ansatz erleichtert die Steuerung gängiger Risiken und ermöglicht eine Verbesserung der Objektivität und der Effizienz. MONARC ist vollständig wiederholbar, deshalb können die Ergebnisse vertieft und an den Reifegrad der jeweiligen Organisation angepasst werden, indem die Granularität der Risikoszenarien erhöht wird.

**Bestimmung des Kontextes**

Diese erste Phase besteht darin, den Kontext, die Herausforderungen und die Prioritäten zu bestimmen, die kennzeichnend für das Unternehmen oder die Organisation sind, das bzw. die eine Risikoanalyse vornehmen möchte.

Es geht darum, insbesondere die wesentlichen Aktivitäten und die kritischen Prozesse des Unternehmens zu identifizieren, um die Risikoanalyse an den wichtigsten Elementen ausrichten zu können. Zu diesem Zweck wird ein Kick-off-Meeting mit den Mitgliedern des Managements und Personen in Schlüsselfunktionen organisiert. Ziel ist es zu erfahren, was die Existenz des Unternehmens ausmacht und was diese vernichten könnte, und die Schlüsselprozesse, die internen und externen Bedrohungen sowie die organisatorischen, technischen und menschlichen Schwachstellen zu identifizieren.

**Modellierung des Kontextes**

Diese Phase beinhaltet die Modellierung der Objektbäume. Die Assets wurden in der Phase davor bestimmt. Sie müssen jetzt in einem Schema detailliert aufgeführt und formalisiert werden, in dem ihre Abhängigkeiten dargestellt sind.

Die Auswirkungen werden auf Ebene der primären Assets (Dienste oder Informationen) bestimmt. Die sekundären Assets erben die Auswirkungen des primären Assets, mit dem sie verknüpft sind (Objektbaum).

Die Auswirkungen auf Ebene der sekundären Assets können manuell angepasst werden.

**Risikobewertung und Risikobehandlung**

Bei der Bewertung geht es darum, die Bedrohungen, die Schwachstellen und die Auswirkungen zu beziffern, damit eine Berechnung der Risiken möglich ist.

Zu diesem Zweck müssen hochwertige Informationen über die genaue Wahrscheinlichkeit der Bedrohungen, die Möglichkeit zur Ausnutzung von Sicherheitslücken und die potenziellen Auswirkungen zur Verfügung stehen. Es sollten daher Kennzahlen herangezogen werden, die von Experten geprüft und bestätigt wurden.

Sollte sich bei der Bewertung der Risiken ergeben, dass ein Risiko über dem akzeptablen Maß liegt (Risikoakzeptanzschema), müssen Maßnahmen zur Behandlung dieses Risikos ergriffen werden, um es auf ein akzeptables Maß zu reduzieren.

**Umsetzung und Monitoring**

An die erste Risikobehandlung schließt sich eine Phase des ständigen Sicherheitsmanagements mit wiederkehrender Kontrolle und Überwachung der Sicherheitsmaßnahmen an, damit diese dauerhaft verbessert werden können.

Diese vierte Phase ermöglicht auch die kontinuierliche Optimierung der Sicherheit durch Erhöhung der Granularität der verwendeten Objekte bzw. durch Erweiterung des Umfangs der Risikoanalysen.

# Bestimmung des Kontextes

## Beschreibung des Kontextes

${CONTEXT\_GEST\_RISK}

## Festlegung der Kriterien für die Risikobewertung

### Skala Auswirkungen

Die nachfolgende Tabelle enthält eine Skala für die Auswirkungen und Konsequenzen, die ein Risiko auf die Einrichtung haben kann. 0 bedeutet „keine Auswirkung“, daher besteht auch kein Risiko.

${SCALE\_IMPACT}

### Skala Bedrohungen

Die nachfolgende Tabelle enthält eine Skala für die Wahrscheinlichkeit, dass sich eine Bedrohung konkretisiert.

${SCALE\_THREAT}

### Skala Sicherheitslücken

Die nachfolgende Tabelle enthält eine Skala, die beschreibt, in welchem Maße das betreffende Asset mit Sicherheitslücken behaftet ist. Bei der Einschätzung der Sicherheitslücken werden die bestehenden Sicherheitsmaßnahmen berücksichtigt.

${SCALE\_VULN}

### Tabelle der Risiken und Risikoakzeptanzschwellen

Die nachfolgende Tabelle enthält die Berechnung der Risiken. Die Farben dienen lediglich der Orientierung und können vom Verwaltungsrat/Führungsgremium übernommen oder geändert werden.

Rot : Inakzeptables Risiko, dem entgegengewirkt werden muss.

Orange: Mittleres Risiko, dem fallabhängig entgegengewirkt werden sollte oder kann.

Grün : Geringes Risiko, das kein Handeln erfordert.

**Risiken der Informationen**

${TABLE\_RISKS}

**Operative Risiken**

${TABLE\_OP\_RISKS}

## Bewertung der Tendenzen und der Bedrohungen

${SYNTH\_EVAL\_THREAT}

In der nachfolgenden Tabelle sind die Bedrohungen aufgeführt, die besonderer Aufmerksamkeit bedürfen.

${TABLE\_THREATS}

# Modellierung des Kontextes

## Identifizierung der Assets

${SYNTH\_ACTIF}

## Identifizierung der Sicherheitslücken

Der Rückgriff auf die MONARC-Modellierung und ihre Objekte ermöglicht die Identifizierung von Sicherheitslücken mit hinreichender Granularität für wiederholte Risikoanalysen.

Es bleibt jedoch den Beratern überlassen, neue kontextabhängige Risiken einzubeziehen, die sie während der Erfüllung ihres Auftrags feststellen.

## Einschätzung der Konsequenzen

In der nachfolgenden Tabelle sind die Auswirkungen für die wesentlichen Assets von ${COMPANY} aufgeführt.

Der Zeitersparnis halber erben alle sekundären Assets, die in die Modellierung der wesentlichen Assets einfließen, standardmäßig diese Auswirkungen; es ist jedoch eine manuelle feinere Anpassung möglich

${IMPACTS\_APPRECIATION}

# Risikobewertung und Risikobehandlung

Das Ergebnis der Beschaffung der verschiedenen Informationen, Codiervorgänge und Bewertungen werden im MONARC-Software verarbeitet und dem Kunden zur Verfügung gestellt. Ein Teil dieser Informationen befindet sich auch im Anhang zu diesem Dokument.

Im weiteren Verlauf dieses Kapitels sind die Ergebnisse und Empfehlungen dargestellt, die den Abschluss dieser Risikoanalyse bilden.

## Zusammenfassung der Risikobewertung

${SUMMARY\_EVAL\_RISK}

${DISTRIB\_EVAL\_RISK}

${GRAPH\_EVAL\_RISK}

## 

## Risikobehandlung

Die nachfolgende Tabelle enthält die wichtigsten Empfehlungen auf Grundlage der Risikoanalyse und des Risikobehandlungsplans. Die Bewertung sowie die Empfehlungen richten sich nach folgender Skala:

●●● : Empfehlung, die ein schnelles Handeln erfordert.

●● : Empfehlung, die ein Handeln erfordert, mit dem einer Sicherheitslücke oder fehlenden Best Practices entgegengewirkt werden soll.

● : Nützlicher Hinweis zur Verbesserung der Sicherheit, Ratschlag.

### Risiken der Informationen

${RISKS\_RECO\_FULL}

### Operative Risiken

${OPRISKS\_RECO\_FULL}

# Anhang A: Interview und Informationsbeschaffung

Die Beschaffung der Informationen, anhand derer die Analyse durchgeführt wird, erfolgt durch Gespräche mit den Schlüsselpersonen des Fachbereichs und den technischen Leitern.

Wir danken den folgenden Personen für ihre aktive Mitwirkung bei den Gesprächen und Besuchen, die im Rahmen unseres Auftrags stattfanden und hier aufgeführt sind:

${TABLE\_INTERVIEW}

# Anhang B: Bewertung der Tendenzen

${TABLE\_EVAL\_TEND}

# Anhang C: Bewertung der Bedrohungen

${TABLE\_THREATS\_FULL}

# Anhang D: Hinweise und Bemerkungen des Beraters

## Risiken der Informationen

${TABLE\_AUDIT\_INSTANCES}

## Operative Risiken

${TABLE\_AUDIT\_RISKS\_OP}