Whitepaper „Risikomanagement in der Informationssicherheit“

Schutzziele: Vertraulichkeit, Integrität, Verfügbarkeit

Version: 1.0
Datum: 31.07.2020
Klassifizierung: öffentlich/public

VDA | Verband der Automobilindustrie

Inhalt

Einleitung und Motivation

Unternehmerische Entscheidungen sind sowohl mit Chancen als auch mit Risiken verbunden. Die Beurteilung, welche Risiken für ein Unternehmen und für die Unternehmenswerte kontrolliert eingegangen werden können, muss systematisch gesteuert werden. Diesen Prozess nennt man Risikomanagement.

Das Risikomanagement befähigt Unternehmen, unter Abwägung der Chancen und Risiken, angemessene Maßnahmen zum Schutz der Unternehmenswerte zu etablieren. Ein funktionierendes Risikomanagement ist damit ein Steuerungsinstrument für das Management und trägt so maßgeblich zum Unternehmenserfolg bei.

Risikomanagement ist ein essentieller Bestandteil der Informationssicherheit und bildet das Rückgrat jedes funktionierenden Informationssicherheits-Managementsystems (ISMS). Mehrere Gesetze (z. B. AktG, EU-DSGVO, IT-Sicherheitsgesetz) sowie gängige Standards und best practices (z. B. ISO/IEC 27001, VDA ISA) fordern ein etabliertes Risikomanagement.

Ziel dieses Whitepapers ist es, Unternehmen in der Automobilindustrie hinsichtlich eines risikoorientierten Informationssicherheits-Managements zu sensibilisieren und zu befähigen, ein effektives Informationssicherheits-Risikomanagement (ISRM) zu etablieren. Informationssicherheitsrisiken bestehen bei der Erstellung und der Verarbeitung von Informationen und beziehen sich auf potenzielle Ereignisse, die einen negativen Effekt auf die Erreichung der Schutzziele der Informationssicherheit haben.

Der Fokus des Whitepapers liegt auf den Schutzzielen Vertraulichkeit, Integrität und Verfügbarkeit. Die Begriffe „Unternehmen“ und „Organisation“ sowie „Informationssicherheitsrisiken“ und „Risiken“ werden nachfolgend synonym verwendet.

Die Ausführungen dieses Whitepapers orientieren sich an den Risikomanagement-Standards ISO 31000 und ISO/IEC 27005, berücksichtigen jedoch spezifische Anforderungen der Automobilindustrie.

Einordnung in den Kontext von TISAX und VDA ISA

Der Verband der Automobilindustrie (VDA) hat 2017 eine einheitliche Methodik zur Bestimmung des Informationssicherheitsniveaus einer Organisation festgelegt. Die Bezeichnung dafür lautet „Trusted Information Security Assessment Exchange“ (TISAX).

Die Basis von TISAX bildet der Anforderungskatalog des VDA, der Information Security Assessment Katalog (VDA ISA). Dieser enthält Kontrollfragen zur Bestimmung des Informationssicherheitsniveaus.

Die mit den Kontrollfragen verbundenen Anforderungen wurden durch eine Risikobeurteilung des VDA Arbeitskreises Informationssicherheit ermittelt und sind als Mindestanforderungen an den Schutz von Informationen, die bei der Zusammenarbeit in der Automobilindustrie verarbeitet werden, zu verstehen.

Der VDA ISA (Version 5.0) enthält eine konkrete Kontrollfrage zum Informationssicherheits-Risikomanagement (1.4.1):

> ***„Inwieweit werden Informationssicherheitsrisiken gemanagt?“***
>
> *„Ziel eines Informationssicherheits-Risikomanagements ist das frühzeitige Erkennen, Bewerten und Behandeln von Risiken zur Erreichung der Schutzziele der Informationssicherheit. Es befähigt damit die Organisation, unter Abwägung der Chancen und Risiken angemessene Maßnahmen zum Schutz der Informationswerte der Organisation zu etablieren. Es ist empfehlenswert, das Informationssicherheits-Risikomanagement einer Organisation so einfach wie möglich zu gestalten, um es effektiv und effizient betreiben zu können.“*

Auflistung 1: Kontrollfrage und deren Ziel gemäß VDA ISA

Die nachfolgenden Empfehlungen sollen eine Hilfestellung für Unternehmen sein, um die Anforderungen aus dieser Kontrollfrage effektiv umzusetzen.

Den Prozessschritten sind jeweils zwei Beispiele zur Veranschaulichung beigefügt. Diese werden über den gesamten Verlauf mitgeführt.

Begriffsdefinitionen

Informationswerte (Information Assets)

Informationswerte stellen schutzwürdige Unternehmenswerte, Prozesse oder Informationen dar. Diese Informationen können in physischer (z. B. Dokumente, Prototypen) und/oder digitaler Form (z. B. als Datei oder in Datenbanken) vorliegen. Das Whitepaper widmet sich insbesondere den Informationen der Automobilindustrie, z. B. Design- und Konstruktionsdaten, Entwicklungs-Know-how oder Logistik-Informationen.

Bedrohung

Eine Bedrohung ist ein Umstand oder Ereignis, welches die Schutzziele der Informationssicherheit beeinträchtigen kann. Die Ursache für eine Bedrohung kann innerhalb oder außerhalb eines Unternehmens ihren Ursprung haben und beabsichtigt oder unbeabsichtigt sein.

Schwachstelle

Eine Schwachstelle ist eine sicherheitsrelevante Lücke in Prozessen, Systemen und/oder Organisationen (z. B. Mitarbeiter). Eine Schwachstelle kann dazu führen, dass eine Bedrohung wirksam wird und ein Schaden entsteht.

Eintrittswahrscheinlichkeit

Die Eintrittswahrscheinlichkeit ist eine Abschätzung für die Häufigkeit, mit der eine Bedrohung eine Schwachstelle ausnutzt.

Schaden

Ein Schaden entsteht durch das Eintreten einer Bedrohung unter Ausnutzung einer Schwachstelle. Dies bedeutet eine negative Auswirkung auf die Organisation.

Risiko

Ein Risiko beschreibt die Kombination aus Bedrohung und Schwachstelle, bewertet hinsichtlich Eintrittswahrscheinlichkeit und potenziellem Schaden. Das Eintreten eines Risikos kann zu einer negativen Abweichung operativer oder strategischer Ziele führen.

Organisatorische Rahmenbedingungen

Festlegung des Geltungsbereichs

Das Risikomanagement der Informationssicherheit orientiert sich am Geltungsbereich des ISMS.

Rollen und Verantwortlichkeiten

Für die Risikobeurteilung und -behandlung werden unterschiedliche Aufgaben, Kompetenzen und Verantwortlichkeiten benötigt. Diese werden typischerweise in Rollen abgebildet. Grundsätzlich und insbesondere in sehr kleinen Organisationen können mehrere Rollen von ein und derselben Person wahrgenommen werden. Bei der Zusammenlegung mehrerer Rollen auf eine Person sollte beachtet werden, dass Interessenskonflikte entstehen können. Diese sollten berücksichtigt werden.

Risikomanager

Der Risikomanager steuert das Risikomanagement im Unternehmen und „behält den Überblick“ über die Risiken. Er konsolidiert die einzelnen Risiken und berichtet diese an die Organisationsleitung. Er legt Prozesse, Methoden, Tools / Templates fest und ist für die Qualitätssicherung gemeldeter Risiken verantwortlich.

Risikoeigner

Der Risikoeigner ist für die Beurteilung und Behandlung der ihm zugeordneten Risiken verantwortlich. Der Risikoeigner muss daher auf einer Hierarchieebene innerhalb der Organisation festgelegt werden, die befugt ist, entsprechende Entscheidungen im Umgang mit Risiken zu treffen. In der Praxis ist es üblich, dass der Risikoeigner aus einer Fachabteilung („Business“) stammt und gleichzeitig der Informationseigner ist. Für die Beurteilung und Behandlung von Risiken sollte er fachliche Expertise aus dem Business hinzuziehen. Die Durchführung der Risikobeurteilung und -behandlung kann seitens des Risikoeigners delegiert werden, niemals jedoch die Verantwortung.

Alle Mitarbeiter und Dritte

Jeder Mitarbeiter oder Dritte, der Zugriff auf Informationen oder auf IT-Systeme der Organisation hat, ist dafür verantwortlich, Bedrohungen, welche die Informationssicherheitsziele gefährden können, zu identifizieren und an den Risikoeigner

(sofern bekannt), den Risikomanager oder Sicherheitsverantwortlichen des Unternehmens zu kommunizieren.

Risikomanagement besteht im Wesentlichen aus den Schritten Risikobeurteilung sowie Risikobehandlung und -überwachung.

Risikobeurteilung

In diesem Kapitel wird erläutert, wie die Anforderungen der Kontrollfrage 1.4.1 des VDA ISA in Bezug den ersten Schritt - die Risikobeurteilung - umgesetzt werden können.

+ Risikobeurteilungen werden sowohl regelmäßig als auch anlassbezogen durchgeführt.

+ Bei Änderung des Umfelds (z. B. Organisationsstruktur, Standort, Änderung von Richtlinien) erfolgt eine zeitnahe Neubewertung.

+ Informationssicherheitsrisiken werden in geeigneter Form gemäß (z. B. Eintrittswahrscheinlichkeit und potenzieller Schaden) bewertet.

+ Es existiert eine Vorgehensweise, wie Informationssicherheitsrisiken innerhalb der Organisation identifiziert, beurteilt und behandelt werden.

+ Informationssicherheitsrisiken sind dokumentiert.

+ Jedem Informationssicherheitsrisiko ist ein Verantwortlicher (Risikoeigner) zugeordnet. Dieser ist für die Beurteilung und Behandlung der Informationssicherheitsrisiken verantwortlich.

Auflistung 2: Maßnahmen gemäß VDA ISA zur Risikobeurteilung

Neben der systematischen Erfassung von Risiken im Rahmen eines regelmäßigen Prozesses ist es erforderlich, dass auch kurzfristig erkannte Risiken anlassbezogen in das Risikomanagement eingesteuert und dokumentiert werden.

Das Ergebnis der Risikobeurteilung ist eine Übersicht („Risikoregister“) aller identifizierten Risiken, die Einordnung in „sehr hohe“, „hohe“, „mittlere“ und „geringe“ Risiken sowie die Zuordnung der Risiken zu den Risikoeignern. Diese Übersicht ist die Basis für den nächsten Schritt - die Risikobehandlung.

Im Folgenden werden die Schritte zur Identifikation, Analyse und Beurteilung von Risiken erläutert und kann - ergänzt um die jeweiligen Verantwortlichkeiten zu den einzelnen Schritten - als Prozessbeschreibung gesehen werden.

Die Risikobeurteilung besteht aus den folgenden Aktivitäten:

1) Risikoidentifikation
2) Risikoanalyse (und -bewertung)

Risikoidentifikation

Zweck der Risikoidentifikation ist die systematische Erfassung der auf eine Organisation einwirkenden Risiken. Mögliche Werkzeuge für die Identifizierung von Risiken sind Workshops (mit Fachexperten) oder Assessments (z. B. ein TISAX Self Assessment mithilfe des VDA ISA).

Die im VDA ISA beschriebenen Anforderungen stellen bei effektiver Umsetzung bereits risikoreduzierende Maßnahmen dar und spiegeln ein akzeptiertes Risikoniveau der Mitglieder des VDA wider. Daher eignet sich ein TISAX Assessment sehr gut, mögliche Abweichungen zu den Anforderungen und somit potenzielle Schwachstellen in der Organisation zu identifizieren.

Im Rahmen der Risikoidentifikation sollten folgende Aspekte betrachtet werden:

- die zu schützenden Informationswerte (Assets)
- relevante Bedrohungen
- potenzielle Schwachstellen

1) Ausgangspunkt: Identifikation der zu schützenden Informationswerte

Mögliche Risiken sollten auf Basis der identifizierten, kritischen Informationswerte erfasst und den jeweiligen Verantwortlichen zugeordnet werden (VDA ISA Kontrollfrage 1.3.1). Gemäß der Kontrollfrage 1.3.2 werden anschließend die identifizierten Informationswerte im Zuge einer Informationsklassifizierung hinsichtlich ihres Schutzbedarfs kategorisiert (siehe VDA „Whitepaper „Harmonisierung der Klassifizierungsstufen“).

Beispiele:

- *Informationswert 1: Wegfahrsperren-relevanten Daten, die von einem Automobilhersteller an einen Lieferanten übertragen werden - sehr hoher Schutzbedarf.*
- *Informationswert 2: Forschungs- und Entwicklungsinformationen in physischer und digitaler Form - hoher Schutzbedarf.*

2) Identifikation von relevanten Bedrohungen

Zur Identifikation von Bedrohungen sollten Meinungen von interne Fachexperten eingeholt, Erfahrungen aus vergangenen Informationssicherheitsvorfällen oder Informationen von IT-Sicherheitsunternehmen oder Behörden berücksichtigt werden. Hierfür können unterstützend standardisierte Bedrohungskataloge (z. B. Bedrohungskatalog des Bundesamts für Sicherheit in der Informationstechnik (BSI), Annex des ISO/IEC 27005) hinzugezogen werden.

Beispiele:

- *Bedrohung 1: Angriff von Hackern*
- *Bedrohung 2: Unberechtigter Zutritt zu Entwicklungsbüros mit krimineller Absicht*

3) Identifikation von potenziellen Schwachstellen

Der dritte Aspekt der Risikoidentifikation ist die Identifikation potenzieller Schwachstellen.

Der VDA ISA verlangt in der Kontrollfrage 5.2.6 die zeitnahe Informationsbeschaffung (z. B. Informationen von IT-Sicherheitsunternehmen) bezüglich potenzieller Schwachstellen und zusätzlich in 5.2.7 die Überprüfung von IT-Systemen auf Schwachstellen. Darüber hinaus sollte die Meinung interner Fachexperten eingeholt oder berücksichtigt werden, um konkrete potenzielle Schwachstellen (je nach Informationswert) zu identifizieren.

Beispiele:

- *Schwachstelle 1: Fehlende Sicherheitspatche in IT-Systemen*
- *Schwachstelle 2: Fehlende Verschlüsselung gespeicherter Daten*
- *Schwachstelle 3: Erteilte Zutrittsberechtigungen werden nicht regelmäßig kontrolliert und nicht automatisch entzogen*

Abschließend werden die Ergebnisse der einzelnen Schritte der Risikoidentifikation kombiniert. Diese Ergebnisse können in Form von Schadens-/Risikoszenarien dargestellt werden.

Beispiele:

- *Risikoszenario 1: Durch einen Angriff von Hackern (Bedrohung 1) auf IT-Systeme mit fehlenden Sicherheitspatchen (Schwachstelle 1) können Wegfahrsperren-relevante Daten (Informationswert 1) gestohlen werden. Der Schaden entsteht, da die Daten nicht verschlüsselt gespeichert werden (Schwachstelle 2)*
- *Risikoszenario 2: Durch unberechtigten Zutritt zu den Entwicklungsbüros (Bedrohung 2) ist ein Diebstahl von Forschungs- und Entwicklungsinformationen in physischer und digitaler Form (Informationswert 2) ist möglich, da einmal vergebene Berechtigungen nicht regelmäßig kontrolliert oder automatisch entzogen werden (Schwachstelle 3), z. B. bei ausscheidenden Mitarbeitern.*

Die so beschriebenen Risiken bilden den Abschluss der Risikoidentifikation und stellen den Input für die Risikoanalyse dar.

Risikoanalyse

Während der Risikoanalyse werden die in der Risikoidentifikation festgestellten Risiken weiter untersucht. Das Ziel ist eine Einschätzung des vorliegenden Risikos in Form von Risikoklassen. Die Berechnung kann zum Beispiel wie folgt geschehen:

Risikoklasse = Eintrittswahrscheinlichkeit x potenzieller Schaden

In einer pragmatischen Form wird der potenzielle Schaden direkt aus der Informationsklassifizierung gemäß der im VDA ISA definierten Schutzklassen („normal“, „hoch“ und „sehr hoch“) übernommen, ergänzt durch die Schutzklasse „niedrig“ (Empfehlung des BSI).

Die Eintrittswahrscheinlichkeit gibt an, wie wahrscheinlich die Schwachstelle ausgenutzt werden wird. Auch hier kann ein vierstufiges Schema, (z. B. „unwahrscheinlich“, „möglich“, „wahrscheinlich“ und „sehr wahrscheinlich“) verwendet werden.

Bei den Eintrittswahrscheinlichkeiten hat sich die Verwendung relativer Häufigkeiten des Eintretens bezogen auf Jahre etabliert:

Eintrittswahrscheinlichkeit	Häufigkeit des Eintretens	Wert
sehr wahrscheinlich	Jährlich oder häufiger	100%
wahrscheinlich	Etwa alle 2 Jahre	50%
Möglich	Etwa alle 5 Jahre	20%
unwahrscheinlich	Etwa alle 10 Jahre	10%

Tabelle 1: Exemplarische Darstellung der Eintrittswahrscheinlichkeiten

Risikobewertung

Die Risikobewertung ermöglicht eine Gewichtung der identifizierten Risiken und damit eine risikoorientierte Vorgehensweise: Bestandsgefährdende Risiken verlangen andere Behandlungs- und Steuerungsmaßnahmen als unwesentliche Risiken. Im Rahmen der Bewertung werden alle identifizierten Risiken analysiert und ihre Eintrittswahrscheinlichkeit sowie ihr Schadensausmaß bewertet.

In Kombination ergibt sich daraus eine 4 x 4 Matrix, aus der die sich ergebende Risikoklasse abgelesen wird. Die Bewertung der einzelnen Felder als „gering“, „mittel“, „hoch“, „sehr hoch“ und deren Farbgebung hängt von der individuellen Organisation ab und deren Bereitschaft, Risiken einzugehen („Risikoappetit“).

Schutzklasse / Eintritts-wahrscheinlichkeit	gering	normal	hoch	sehr hoch
sehr wahrscheinlich	gering	mittel	hoch	sehr hoch
wahrscheinlich	gering	mittel	hoch	hoch
möglich	gering	gering	mittel	mittel
unwahrscheinlich	gering	gering	gering	gering

Tabelle 2: Exemplarische Darstellung einer 4 x 4 Risikomatrix (Basis: BSI)

Die Einstufung des Risikos in die entsprechende Risikoklasse („gering“, „mittel“, „hoch“ oder „sehr hoch“) stellt somit die Risikobewertung dar und bildet den Abschluss der Risikobeurteilung. Die Risikobewertung stellt einen bewussten Entscheidungsvorgang durch den Risikoeigner dar.

Aus der Identifikation, Analyse und Bewertung der Risiken resultiert das Risikoregister mit den nach Risikoklassen priorisierten Risiken. Im Anschluss muss entschieden werden, wie mit den Risiken umgegangen wird. Diese Risikobehandlung wird im Risikobehandlungsplan dokumentiert.

Beispiele

- *Risikoszenario 1: Die Eintrittswahrscheinlichkeit eines Angriffs auf IT-Systeme mit fehlenden Sicherheitspatchen wird durch Fachexperten als „sehr wahrscheinlich“ bewertet. Für die Wegfahrsperren-relevanten Daten wurde in der Informationsklassifizierung bereits ein „sehr hoher“ Schutzbedarf festgestellt, die Risikoklasse ist daher als „sehr hoch“ zu bewerten.*
- *Risikoszenario 2: Die Eintrittswahrscheinlichkeit eines unberechtigten Zutritts zu Entwicklungsbüros wurde als „wahrscheinlich“ bewertet. Der Zutritt zu den Büros erfolgt über eine Schlüsselkarten-Leser gesteuerte Tür oder einen Schlüssel/Schließzylinder. Auswertungen haben ergeben, dass mehrere bereits ausgeschiedene Mitarbeiter noch Zutrittsberechtigungen haben und der Verbleib zweier Schlüssel nicht geklärt werden konnte. Für die Forschungs- und Entwicklungsinformationen in physischer und digitaler Form wurde in der Informationsklassifizierung ein „hoher“ Schutzbedarf festgestellt, die Risikoklasse ist als „hoch“ zu bewerten.*

Da die Risikoklasse des Risikoszenarios 1 („sehr hoch“) höher als der Risikoklasse des Risikoszenarios 2 („hoch“) ist, ist das Risikoszenario 1 in der nachfolgenden Risikobehandlung zu priorisieren. Die priorisierten Risiken werden in das Risikoregister eingetragen.

Risikoszenario	Risikoklasse	Prio	Risikoeigner
Diebstahl von Wegfahrsperren-relevante Daten	sehr hoch	1	Person A
Unberechtigter Zutritt zu und Entwicklerbüros	hoch	2	Person B

Tabelle 3: Exemplarische Darstellung eines Risikoregisters

Für jedes Risiko muss ein Risikoeigner bestimmt und dokumentiert werden. In der Regel ist dies der Informationseigner.

Risikobehandlung

Dieses Kapitel erläutert, wie die Anforderungen der VDA ISA Kontrollfrage 1.4.1 in Bezug auf den zweiten Schritt - der Risikobehandlung - umgesetzt werden können.

+ Kriterien für die Beurteilung und Behandlung von Informationssicherheitsrisiken sind vorhanden.

+ Maßnahmen zur Behandlung von Informationssicherheitsrisiken und deren Verantwortliche sind festgelegt und dokumentiert.

- Es existiert ein Maßnahmenplan bzw. Statusübersicht der Maßnahmenumsetzung.

Auflistung 3: Maßnahmen gemäß VDA ISA zur Risikobehandlung

Risiken müssen entsprechend ihrer Bewertung adäquat behandelt werden. Die Grundlage hierfür bildet das Risikoregister.

Es gibt unterschiedliche Wege, mit einem Risiko umzugehen. Grundsätzlich wird zwischen vier Arten der Risikobehandlung unterschieden:

- Risikoeliminierung (Vermeidung, engl. Avoidance)
- Risikoreduktion (Kontrolle, engl. Mitigation)
- Risikotransfer (Übertragung, engl. Transfer)
- Risikoübernahme (Akzeptanz, engl. Acceptance)

Um ein akzeptables Restrisikoniveau (Risikoklasse nach effektiver Behandlung) zu erreichen, kann die Behandlung eines Risikos auf eine oder mehrere Arten erfolgen. Der Risikoeigner entscheidet über die Art der Risikobehandlung.

Risikoeliminierung

Eine Eliminierung bzw. eine komplette Vermeidung des Risikos erfolgt, wenn Aktivitäten oder Vorgänge, welche das Risiko verursachen (z. B. ein Projekt zum Aufbau eines neuen Standorts, eine neue Produktvariante oder Dienstreisen in eine bestimmte Region) gänzlich gestoppt bzw. eliminiert werden. Damit wird eine Bedrohung nicht mehr zum Risiko.

Risikoreduktion

Die Risikoreduktion ist die am häufigsten gewählte Art der Risikobehandlung. Eine Reduktion des Risikos kann z. B. durch eine oder mehrere, sich ergänzende Maßnahmen erfolgen, die dem Risiko entgegenwirken. Hierbei wird die Eintrittswahrscheinlichkeit eines potenziellen Schadens und/oder dessen Schadensausmaß durch Sicherheitsmaßnahmen verringert. Risikoreduzierende Maßnahmen können technischer oder organisatorischer/prozessualer Art (z. B. Durchführung von Sicherheitstrainings, Umstrukturierung von Prozessen/Abläufen, bauliche Maßnahmen) sein.

Risikotransfer

Bei einem Risikotransfer wird der potenzielle Schaden durch einen anderen Verantwortungsbereich oder eine andere Institution getragen. Dies kann zum Beispiel durch Outsourcing oder – als Vorbeugung gegen finanzielle Risiken – durch den Abschluss von Versicherungen (z. B. Ausfallversicherung, Cyber Security Insurance) erfolgen. Die Verantwortung für das Risiko verbleibt beim Risikoeigner innerhalb der Organisation.

Risikoübernahme (Akzeptanz)

Im Rahmen der Risikoübernahme werden die Risiken in ihrer vorliegenden Risikoklasse akzeptiert.

Die Risikoübernahme kann eine geeignete Vorgehensweise sein, wenn die Geschäftschancen größer sind als die Risiken oder wenn Maßnahmen fehlen, die das Risiko finanziell effizient reduzieren können. Verstöße gegen Gesetze (mit z. B. möglichen straf- oder zivilrechtliche Konsequenzen) dürfen generell nicht mittels Risikoakzeptanz übernommen werden.

Risikoübernahmen dürfen nur durch Risikoeigner erfolgen, deren finanzielle Verantwortung der jeweiligen Risikoklasse zumindest entspricht.

Da eine Risikoübernahme Folgen über den betrachteten Bereich hinaus haben kann, müssen organisationsweite Regelungen und Vorgaben (z. B. Schwellwerte für die Akzeptanz von Risiken, Wesentlichkeitsgrenzen) definiert werden. Damit soll unter anderem vermieden werden, dass ein Risikoeigner ein Risiko akzeptiert, das für die gesamte Organisation kritisch sein kann.

In diesem Fall muss die Leitung der Organisation (z. B. Geschäftsführung/Vorstand) informiert und in die Entscheidung einbezogen werden bzw. diese idealerweise selbst treffen.

Die Übernahme eines Risikos, dessen Risikoklasse eine definierte Schwelle überschreitet, muss in Form eines Risikoübernahmeformulars dokumentiert werden.

Für Risiken, die sich aus einer Abweichung von den abgestimmten Anforderungen der Automobilindustrie (VDA ISA) ergeben, ist eine Risikoakzeptanz seitens einer Organisation nicht möglich.

Risikobehandlungsplan

Die Handhabung jedes einzelnen Informationssicherheitsrisikos wird in einem Risikobehandlungsplan (engl. Risk Treatment Plan) definiert. Dort wird festgehalten, wie mit dem jeweiligen bewerteten Risiko umgegangen wird, wer verantwortlich für die Umsetzung ist sowie bis wann die Umsetzung zu erfolgen hat.

Beispiele:

- *Risikoszenario 1: Der Risikoeigner entscheidet sich für Risikoreduzierung durch Patchen aller betroffenen IT-Systeme (Maßnahme 1) und Installation einer Verschlüsselung auf relevanten IT-Systemen und Datenträgern (Maßnahme 2), die für die Verarbeitung der Wegfahrsperren-relevanten Daten genutzt werden.*
- *Risikoszenario 2: Der Risikoeigner würde das Risiko gerne akzeptieren und keine weiteren Maßnahmen zur Risikobehandlung unternehmen. Da in den Räumlichkeiten der Forschung und Entwicklung im Rahmen von Projekten jedoch Kundendaten betroffen sein könnten, ist die Risikoakzeptanz nicht möglich und das Risiko muss reduziert werden. Der Risikoeigner entscheidet sich daraufhin für den Austausch des Schließzylinders und aller Schlüssel (Maßnahme 3) sowie für den Entzug aller veralteten Zutrittsberechtigungen (Maßnahme 4).*

Die Verantwortlichkeiten für alle Maßnahmen werden festgelegt und Zeiträume zur Umsetzung vereinbart. Die Maßnahmen werden in das Risikoregister und den Risikobehandlungsplan eingetragen.

Risikoszenario	Risiko-klasse	Risikoeig-ner	Maßnahme	Verantwortlicher, Umsetzungszeit-raum
Diebstahl von Wegfahr-sperren-relevante Daten	sehr hoch	Person A	Patchen der IT-Sys-teme	Person 1 2 Wochen
Diebstahl von Wegfahr-sperren-relevante Daten	sehr hoch	Person A	Verschlüsselung der Daten	Person 2 2 Wochen
Unberechtigter Zutritt zu und Entwicklerbüros	hoch	Person B	Austausch Schlüs-sel und Schließzy-linder	Person 3 4 Wochen
Unberechtigter Zutritt zu und Entwicklerbüros	hoch	Person B	Entzug veralteter Zutrittsberechtigun-gen	Person 4 2 Wochen

Tabelle 4: Exemplarische Darstellung eines Risikobehandlungsplans

Risikoüberwachung und -kommunikation

Nachverfolgung der Risiken und Umsetzung der Behandlungspläne

Ein funktionierendes Risikomanagement erfordert die effektive Behandlung von Risiken.

Aus diesem Grund muss ein Prozess etabliert werden, der die Nachverfolgung von umzusetzenden Maßnahmen ermöglicht und bei Verzögerung oder bei Nichtbehandlung von Risiken Möglichkeiten zum Gegensteuern bietet. Dazu gehören mindestens die folgenden Punkte:

- Verwaltung und Kontrolle der Behandlungspläne möglichst einheitlich und zentral (z. B. Datenbank oder Kollaborationsplattform)
- Eindeutige Verantwortlichkeiten festlegen (wer ist für die Umsetzung welcher Maßnahme in welchem Zeitraum verantwortlich)
- Regelmäßige Kontrolle des Fortschritts
- Festgelegte Kommunikations- und Eskalationswege
- Folgen bei Nichtumsetzung (z. B. Eskalation an die nächsthöhere Managementebene, ggf. Risikoakzeptanz)
- Fester Bestandteil interner und externer Audits

An dieser Stelle kommt besonders das Risikobewusstsein des Managements zum Tragen. Bei mangelhafter Umsetzung von Behandlungsplänen muss das Management nach Kenntnisnahme reagieren.

Dokumentation und Berichterstattung / Reporting

Die in diesem Whitepaper beschriebenen Ansätze und Maßnahmen (z. B. Rollen und Verantwortlichkeiten, Geltungsbereich, Risikomanagementprozess) sind zu dokumentieren. Hierbei kann es sinnvoll sein, sich an gegebenenfalls bereits bestehende Risikomanagement-Ansätze oder -Systeme anzuschließen bzw. diese zusammenzuführen (z. B. Umweltmanagement, Qualitätsmanagement, Compliance). Die wesentlichen Ergebnisse des Risikomanagements sollten regelmäßig an die Organisationsleitung berichtet werden.

Beispiele

- *Risikoszenario 1: Die Maßnahmen 1 (Patchen) und 2 (Verschlüsselung) werden zeitgerecht von den Umsetzungsverantwortlichen zurückgemeldet. Die Risikoklasse reduziert sich durch die Effektivität der umgesetzten Maßnahmen auf „gering“ (Eintrittswahrscheinlichkeit „unwahrscheinlich“ und Schutzklasse „sehr hoch“).*
- *Risikoszenario 2: Die Maßnahme 4 (Entzug alter Zutrittsberechtigungen) wird zeitgerecht vom Umsetzungsverantwortlichen zurückgemeldet. Die Maßnahme 3 (Austausch des Schließzylinders und aller Schlüssel) wird nicht zeitgerecht umgesetzt. Nach einer Eskalation seitens des Risikomanagers über die Organisationsleitung wird die Maßnahme mit verlängerter Umsetzungsfrist abgeschlossen. Nach Umsetzung aller Maßnahmen verringert sich die Risikoklasse auf „gering“ (Eintrittswahrscheinlichkeit „unwahrscheinlich“ und Schutzklasse „hoch“). Die Maßnahme wird weiter überwacht.*

Risikoszenario	Risiko-klasse	Risiko-eigner	Beschreibung
Diebstahl von Wegfahrsperren-relevante Daten	gering	Person A	Umsetzung der Maßnahmen 1 und 2 ist am xx.xx.xxxx erfolgt. Die Risikoklasse reduziert sich damit auf „gering“
Unberechtigter Zutritt zu und Entwicklerbüros	gering	Person B	Umsetzung der Maßnahmen 4 ist am xx.xx.xxxx erfolgt. Umsetzungsfrist Maßnahme 3 verlängert nach Freigabe/Risikoakzeptanz Organisationsleitung bis xx.xx.xxxx

Tabelle 5: Exemplarische Darstellung des angepasstne Risikoregisters

Fazit und Empfehlung

Das Whitepaper soll Organisationen bei der Vorbereitung oder Durchführung eines TISAX Assessments unterstützen, die Anforderungen der VDA ISA Kontrollfrage 1.4.1 zu erfüllen. Es ist in diesem Zusammenhang als Umsetzungsempfehlungen zu verstehen, nicht als verpflichtende Vorgabe.

Das ISRM einer Organisation sollte so einfach wie möglich gestaltet werden, um effektiv und auch effizient betrieben werden zu können. Hier spielen auch die Mitarbeiter einer Organisation eine entscheidende Rolle. Denn sie müssen wissen, wie Risiken identifiziert und gemeldet werden können.

Es ist darüber hinaus wichtig, dass sich der ISRM-Prozess an die spezifischen Bedarfe der eigenen Organisation orientiert und in ggf. bereits bestehende Risikomanagement-Systeme integriert wird, auch wenn die meisten der in der Informationssicherheit identifizierten Risiken die Schwellwerte eines Risikomanagements nicht erreichen.

Die Festlegung von klaren Verantwortlichkeiten ist ein weiterer kritischer Erfolgsfaktor des ISRM. Für jedes dokumentierte Risiko sollte ein konkreter Risikoeigner bestimmt werden, damit keine Diskussionen in Bezug auf die Verantwortung bei der Risikobehandlung entstehen. Denn die richtige und gesteuerte Behandlung von Informationssicherheitsrisiken ist entscheidend, damit bei einem tatsächlichen Eintritt eines Risikos die daraus resultierenden Auswirkungen begrenzt werden.

Der VDA empfiehlt seinen Mitgliedern, sich an diesem Whitepaper zu orientieren.

Autorenverzeichnis

Name	Unternehmen	E-Mail-Adresse
Jens Frölich	AUDI AG	jens.froelich@audi.de
Thomas Donner	BMW AG	thomas.donner@bmwgroup.com
Oliver Schmitt	Robert Bosch GmbH	oliver.schmitt@de.bosch.com
Jürgen Rilling	Daimler AG	juergen.rilling@daimler.com
Thomas Harich	MAHLE GmbH	thomas.harich@mahle.com
Matthias Teuscher	Rheinmetall AG	matthias.teuscher@de.rheinmetall.com
Burkhard Kesting	ZF Friedrichshafen AG	burkhard.kesting@zf.com

Dokumenten- und Versionshistorie

Version	Datum	Status, Anmerkungen
1.0	31.07.2020	Final