Informationssicherheit

Übergreifende Richtlinien und Prozesse

Regelung Nr. 03.01.15

Risikomanagement in der Informationssicherheit

Klassifikation: Intern – KSU 2.1

Geltungsbereich: Die Regelungen gelten für die AUDI BRUSSELS

Version 1.1

Inhalt

I. Zweck

Der Zweck dieser Regelung ist das frühzeitige Erkennen und Melden von IT-Sicherheitsrisiken, um die vorhandenen IT-Sicherheitsrisiken transparent zu machen und Abschwächungsmaßnahmen für IT-Sicherheitsrisiken zu definieren.

1. Risikomanagement in der IT-Sicherheit

Das Management der Informationssicherheitsrisiken ist ein essenzieller Teil des Information Security Management System (ISMS). Die Entscheidung über die innerhalb des ISMS zu ergreifenden Maßnahmen muss auf den Informationssicherheitsrisiken basieren. Die IT-Sicherheitsrisiken sind Bestandteil der Informationssicherheitsrisiken und fließen im Rahmen der IT-Risiken in das Risikomanagement des Unternehmens ein.

1.1. Ziel

Das Ziel dieses Kapitels ist die Definition von Anforderungen für das Risikomanagement in der IT-Sicherheit innerhalb der AUDI BRUSSELS.

1.2. Allgemeine Anforderungen

- IT-Sicherheitsrisiken müssen erkannt, dokumentiert und bewertet werden.
- Es muss ein Prozess definiert werden, der folgende Aspekte berücksichtigt:
  - Wann eine Bewertung der IT-Sicherheitsrisiken durchgeführt werden muss und wie diese Objekte erkannt werden können.
  - Definition von Rollen und Verantwortlichkeiten (auch bezüglich der Managementaktivitäten)
- Jedem IT-Sicherheitsrisiko muss ein verantwortlicher Manager als ein Risikoeigner zugewiesen werden.
- Durch geeignete Maßnahmen ist sicher zu stellen, dass jeder Mitarbeiter ihm bekannte potenzielle IT-Sicherheitsrisiken der verantwortlichen Stelle[1] oder seiner zuständigen Führungskraft meldet.
- Im Falle von identifizierten oder gemeldeten Risiken muss die verantwortliche Stelle[2] diese prüfen und entscheiden, ob und wann eine Risikobewertung initiiert wird.
- Für Projekte ist grundsätzlich ein IT-Sicherheitskonzept vorzulegen. In Abhängigkeit der Datenklassifikation ist eine Prüfung der Konzepte durchzuführen.
- Vor der Produktivsetzung eines IT-Systems / Applikation dürfen keine mittlere Risiken (oder höher) mehr vorliegen. In Sonderfällen muss durch geeignete Prozesse das Risiko durch das verantwortliche Management übernommen werden. Eine Risikoreduzierung durch geeignete Maßnahmen muss geprüft werden.

[1] Siehe Anhang B.1.1

[2] Siehe Anhang B.1.1

- Durch geeignete Eskalationsmaßnahmen ist sicher zu stellen, dass mittlere Risiken (oder höher) bei laufenden IT-Systemen / Applikationen dem verantwortlichen Management transparent dargestellt werden und diese zeitnah beseitigt werden.
- Vorhandene Risikobewertungen müssen abhängig von deren Datenklassifikation in angemessenen Zeitabständen überprüft werden.

1.3. Verantwortlichkeiten

- Der CISO ist der Hauptansprechpartner für die Geschäftsprozesseigner zum Thema IT-Sicherheit.
- Um die IT-Sicherheitsrisiken entsprechend identifizieren, bewerten und behandeln zu können, müssen neben dem Prozess auch Rollen definiert und etabliert werden. Wo sinnvoll muss auf ein 4-Augen-Prinzip geachtet werden.

1.4. Management Prozess für IT-Sicherheitsrisiken

1.4.1 Identifikation von IT-Sicherheitsrisiken

- Im Unternehmen muss ein Prozess[3] existieren, der die Identifikation von IT-Sicherheitsrisiken behandelt
- Für die Risikoidentifikation müssen je nach Datenklassifikation oder Schutzbedarf folgende Informationsquellen verwendet werden:
  - Ergebnisse aus dem IT Service Continuity Management-Prozess[4]
  - Ergebnisse aus dem IT-Sicherheitsvorfall-Prozess[5]
  - Gemeldete Schwachstellen (z. B. vom Hersteller oder von Mitarbeitern gemeldete Schwachstellen)
  - Schwachstellen-Scans
  - Ergebnisse aus Audits (intern und extern)
  - Ergebnisse aus Penetrationstests
  - Maßnahmen aus Audits
  - IT-Sicherheits-Risiko-Analysen von Applikationen
  - Abweichungen vom Informationssicherheits-Regelwerk
- Nach der Identifikation müssen die IT-Sicherheitsrisiken zur weiteren Behandlung genau beschrieben und dokumentiert werden.

1.4.2 Bewertung von IT-Sicherheitsrisiken

- IT-Sicherheitsrisiken müssen analysiert und bewertet werden. Hierbei sollte der Schaden und die Eintrittswahrscheinlichkeit berücksichtigt werden.

---

[3] Siehe Anlage A.1.3

[4] wie in Informationssicherheit Regelung Nr. 03.01.14 IT Service Continuity Management (Kapitel 1.3.10) beschrieben

[5] wie in Informationssicherheit Regelung Nr. 03.01.18 Informationssicherheitsvorfalls- und Schwachstellenmanagement beschrieben

- Es müssen sowohl Brutto-[6] als auch Nettorisiken (Restrisiken)[7] bewertet werden.
- Implementierte Gegenmaßnahmen müssen bei der Bewertung von Risiken in Betracht gezogen werden.
- Die entsprechenden Experten aus der IT-Organisationseinheit sowie Experten aus den relevanten Nicht-IT-Organisationseinheit müssen hinzugezogen werden, um die potenziellen geschäftlichen Auswirkungen des IT-Sicherheitsrisikos zu bewerten.

1.4.3 Risikobehandlung und Risikoreduzierung (Umsetzungsplan)

- Nachdem IT-Sicherheitsrisiken identifiziert und bewertet wurden, müssen die Risikoeigner in Korrelation mit anderen bekannten Risiken und geplanten/implementierten Maßnahmen dafür Sorge tragen, dass adäquate Maßnahmen zur Sicherstellung einer angemessen und zeitnahen Behandlung der IT-Sicherheitsrisiken getroffen werden. Die Behandlung der Risiken muss mit der für IT-Sicherheit abgestimmt sein.
- Beispiele für Strategien zum Umgang mit IT-Sicherheitsrisiken:
  - Risikovermeidung
  - Risikoreduktion
  - Risikotransfer (z.B. durch Versicherungen)
  - Risikoübernahme
- Der Risikoeigner muss für jede definierte Gegenmaßnahme eine Umsetzungsfrist und -priorität angeben, zusätzlich zu weiteren Organisationseinheiten oder Rollen, falls erforderlich.
- Gegenmaßnahmen müssen gemäß der Effizienz und Risikoreduktionsintensität bewertet werden. Falls erforderlich, müssen betroffene Organisationseinheiten und Experten konsultiert werden, um die Gegenmaßnahmen zu identifizieren, die am besten zur Unternehmensumgebung passen.
- Bei der Auswahl der Strategie und der Zeitdauer der Umsetzung von Maßnahmen bezüglich identifizierter IT-Sicherheitsrisiken muss unter anderem die Einstufung (z. B. niedrig/mittel/hoch) des Risikos beachtet werden.
- Die Gegenmaßnahmen müssen gemäß dem abgestimmten Plan umgesetzt werden.
- Der Risikoeigner ist für die Umsetzung von Maßnahmen gemäß dem Zeitplan und den Anforderungsspezifikationen verantwortlich.
- Die Umsetzung der Gegenmaßnahmen muss bis zu deren Abschluss durch die verantwortliche Stelle[8] überwacht und ggf. eskaliert werden.

[6] Siehe Anhang A.5

[7] Siehe Anhang A.5

[8] Siehe Anhang B.1.1

1.4.4 Effektivitätstest

- Verantwortliche für eine Gegenmaßnahme müssen regelmäßig überprüfen, ob definierte Gegenmaßnahmen für die Reduktion von IT-Sicherheitsrisiken dokumentiert werden und ob diese noch für die Reduktion von IT-Sicherheitsrisiken auf eine festgelegte Stufe geeignet sind und effektiv sind.
- Der Überprüfungszeitraum muss so ausgewählt werden, dass potentielle Abweichungen der Gegenmaßnahmen zur Risikoreduktion erkannt werden können ohne dass diese das Risiko wieder auf das Niveau vor der Gegenmaßnahme erhöhen.

1.4.5 Melden von IT-Sicherheitsrisiken

- Ein IT-Sicherheitsrisiko muss dem CISO der AUDI BRUSSELS gemeldet werden.
- Hat ein identifiziertes Risiko Auswirkungen auf andere Gesellschaften und ist das Restrisiko entsprechend hoch eingestuft worden, so sollten die betroffenen Stellen der Gesellschaften informiert werden.
- Der Risikoverantwortliche[9] muss IT-Sicherheitsrisiken als Bestandteil der Informationssicherheitsrisiken bewerten und entsprechend der Vorgaben des Risikomanagements des Unternehmens melden.

[9] Siehe Anhang B.1.2

II. Verantwortlichkeiten

II.I Kapitel 1: Risikomanagement

Diese Regelung ist von allen Mitarbeitern einzuhalten.

Abweichungen von dieser Regelung, die das Sicherheitsniveau senken, sind nur in Abstimmung mit der IT-Sicherheit und grundsätzlich nur zeitlich begrenzt zulässig.

Anhang

A. Allgemeines

A.1 Mitgeltende Dokumente

A.1.1 Informationssicherheit Regelung Nr. 03.01.09 Ausnahmeprozess

A.1.2 Informationssicherheitshandlungsleitlinien für Mitarbeiterinnen und Mitarbeiter

A.1.3 PS_UP4_FP.05-Information-Security-Risk-Management

A.2 Referenzen zu Standards

Die folgende Tabelle zeigt die Referenzen zu den Standards ISO/IEC 27001:2013, ISO/IEC 27001:2005 und VDA.

Thema	Kapitel	ISO 27001:2013	ISO 27001:2005	VDA
Actions to address risks and opportunities	1	Clause 6.1	Clauses 4.2.1, 4.2.3, 4.3.1, 5.1, 7.2, 8.3	1.2
Information security risk assessment	1.4	Clause 8.2	Clauses 4.2.3, 4.3.1	1.2
Information security risk treatment	1.4	Clause 8.3	Clauses 4.2.2, 4.3.3	

A.3 Anlagen

A.3.1 Anlage 1 Feedbackformular

Das Feedbackformular für Änderungsvorschläge zu Regelungen kann von der MyNet-Webseite Gesellschaften → Audi Brussels → Organisation → Finanz (B/F) → IT (B/FP) → IT-Sicherheit → Regelwerk heruntergeladen werden.

Das Feedback-Formular ist folgendermaßen auszufüllen:

Die Spalten 2 bis 6 müssen für jede vorgeschlagene Änderung ausgefüllt werden. Änderungen, für die nicht alle Spalten 2 bis 6 ausgefüllt sind, werden automatisch ohne weitere Prüfung abgelehnt.

Spalte 3: Folgende Kommentararten sind möglich: a=allgemein, f=fachlich, r=redaktionell

Spalte 4: Bitte bisherigen Text, Tabelle oder Bild einfügen

Spalte 5: Bitte vollständig umformulierten Text, geänderte Tabelle oder geändertes Bild einfügen

Spalte 6: Bitte begründen Sie die gewünschte Änderung möglichst ausführlich.

Bitte senden Sie das ausgefüllte Formular an: it-security.audibx@audi.de

A.4 Quellen und Referenzen

- Standard ISO/IEC 27005:2011 Risikomanagement in der IT-Sicherheit

A.5 Abkürzungen und Definitionen

Abbreviation / Term	Definition
CIO	Chief Information Officer
CISO	Chief Information Security Officer
Bruttorisiko	Das Bruttorisiko ist die aktuelle Bewertung eines IT-Risikos. Das Bruttorisiko umfasst nur abmildernde Aktionen oder Gegenmaßnahmen, die es bereits gibt bzw. die bereits eingeleitet wurden. Darunter fallen keine geplanten oder vorgeschlagenen Aktivitäten oder Gegenmaßnahmen.
IT-Sicherheitsrisiko	Möglichkeit, dass eine gegebene Bedrohung eine Schwachstelle eines Wertes oder eine Gruppe von Werten ausnutzt und dabei Schaden für die Organisation verursacht.
ITRM	IT-Risikomanagement
Nettorisiko	In das Nettorisiko fließen die Gegenmaßnahmen ein, die entweder die tatsächliche Wahrscheinlichkeit oder den materiellen Verlust eines IT-Risikos (oder beides gleichzeitig) vermindern. Damit wird die zukünftige Situation eines IT-Risikos dargestellt, nachdem definierte Gegenmaßnahmen vollständig implementiert wurden.

A.6 Gültigkeit

Diese Regelung ist mit der Veröffentlichung sofort gültig.

Bereits bestehende Ausnahmeregelungen sind spätestens bei der nächsten Änderung (z.B. Verlängerung, Änderung der Auflagen) an diese Regelung anzupassen.

Nächster Überprüfungstermin: 01.10.2023

Für die Meldung von Änderungswünschen verwenden Sie bitte das vorgegebene Formular[10].

A.7 Dokumentenhistorie

Version	Name	Org.-Einheit	Datum	Bemerkung
1.0	Andreas Walter	B/FP	07.08.2019	Veröffentlicht
1.1	Andreas Walter	B/FP	01.10.2020	Anpassung wegen Revisionsvorgaben

[10] Siehe Anhang A.3.1 Anlage 1 Feedbackformular

B. Spezifische Ausprägungen

B.1 Kapitel 1: Risikomanagement

B.1.1 IT-Sicherheit

B.1.2 Definition gemäß URLB_006 Anlage 1