Informationssicherheit

Übergreifende Richtlinien und Prozesse

Regelung Nr. 03.01.08

Change- und Patch-Management

Klassifikation: Intern – KSU 2.1

Geltungsbereich: Die Regelungen gelten für die AUDI BRUSSELS

Version 1.0

Inhalt

I. Zweck

Der Zweck dieser Regelung ist die Definition von Sicherheitsanforderungen an das Change und Patch Management.

1. Change und Patch Management

1.1. Ziel

Das Ziel dieses Kapitels ist die Definition erforderlicher Sicherheitsanforderungen an den Betrieb von IT-Systemen und Anwendungen im Zusammenhang mit Change und Patch Management. Für den sicheren und zuverlässigen Betrieb sind geeignete Verfahren zur Änderungskontrolle und Patch-Prozesse erforderlich.

1.2. Anforderungen an das Change Management

1.2.1 Allgemeine Anforderungen

- Ein geeigneter allgemeiner Change-Management-Prozesses[1] muss definiert und dokumentiert werden.
- Der allgemeine Change-Management-Prozess muss zumindest die Schritte des regulären Change-Prozess[2] und des Notfall-Change-Prozess[3] umfassen.
- Für jedes IT-System muss ein geeigneter Change-Management-Prozess[4] definiert und dokumentiert werden. Es sollte, soweit möglich, der allgemeine Change-Management-Prozess Anwendung finden.
- Für jeden Schritt des allgemeinen Change-Management-Prozess und der spezifischen Change-Management-Prozesse für bestimmte IT-Systeme müssen die jeweiligen Zuständigkeiten definiert werden (Wer ist autorisiert, Changes zu beantragen; welche Einheit ist für die Bearbeitung des Changes zuständig etc.).
- Jeder einzelne Schritt des allgemeinen Change-Management-Prozess und der spezifischen Change-Management-Prozesse für bestimmte IT-Systeme muss im Detail beschrieben werden, damit sich alle betroffenen Einheiten ihrer Aufgaben innerhalb des Prozesses bewusst sind.
- Jeder Change muss genau dokumentiert werden. Diese umfasst die Beantragung, die Klassifikation, die einzelnen Schritte der Planungs- und Vorbereitungsphase, die Freigabe, die während der Umsetzung durchgeführten Schritte sowie die Aktivitäten innerhalb der finalen Prüfungsphase.
- Wenn notwendig, muss nach der Umsetzung des Changes eine Anpassung der System- und Notfalldokumentation erfolgen.

[1] Siehe Anhang B.1.1

[2] Siehe Kapitel 1.2.2

[3] Siehe Kapitel 1.2.3

[4] Siehe Anhang B.1.1

1.2.2 Regulärer Change-Prozess

Der reguläre Change-Prozess umfasst zumindest folgende Schritte:

- Beantragung: Der Antragsteller fordert bei der zuständigen Einheit einen Change für ein System an.
- Prüfung des Change-Antrags: Der Change muss von der zuständigen Einheit auf Vollständigkeit der benötigten Informationen und Notwendigkeit hin geprüft werden.
- Klassifikation des Changes: Changes müssen verschiedenen Klassen[5] zugewiesen werden. Handelt es sich bei einem Change um einen Notfall-Change müssen die Schritte des Notfall-Change-Prozess[6] befolgt werden.
- Planung und Vorbereitung des Changes: Die für die Umsetzung des Changes notwendigen Schritte müssen geplant und vorbereitet werden. Darunter fallen folgende Punkte:
  - Festlegung eines Umsetzungsdatums
  - Identifizierung und Benachrichtigung der durch den Change betroffenen Parteien
  - Analyse des möglicherweise aus der Umsetzung des Changes resultierenden Risikos
  - Durchführung notwendiger Tests
  - Definition der für die Umsetzung erforderlichen Schritte
  - Prüfung auf Erfüllung der Anforderungen an die Informationssicherheit
  - Definition eines Fallback-Konzepts
- Freigabe des Changes: Die Freigabe erfolgt auf der Grundlage der erfolgreichen Durchführung der oben genannten Schritte. Darüber hinaus muss die zuständige Einheit den Change auf Notwendigkeit, finanzielle Angemessenheit und Verfügbarkeit der für die Umsetzung erforderlichen personellen Ressourcen hin prüfen.
- Umsetzung des Changes: Nach der Freigabe erfolgt die Umsetzung seitens der zuständigen Einheit gemäß den definierten Schritten (siehe Abschnitt „Planung und Vorbereitung des Changes“).
- Finale Prüfung des Changes: Nach der Umsetzung erfolgt eine Prüfung des Changes und seiner Auswirkungen. War der Change erfolgreich, ist der Prozess an dieser Stelle beendet. War er nicht erfolgreich, müssen zusätzliche Maßnahmen definiert werden oder das Fallback-Konzept muss zur Anwendung kommen.

1.2.3 Notfall-Change-Prozess

- Beantragung: Der Antragsteller fordert bei der zuständigen Einheit einen Change für ein System an.
- Klassifikation des Changes: Der Change wird als Notfall-Change eingestuft[7].

[5] Siehe Kapitel 1.2.4

[6] Siehe Kapitel 1.2.3

[7] Siehe Kapitel 1.2.4

- Planung und Vorbereitung des Notfall-Changes: Die für die Umsetzung des Changes notwendigen Schritte müssen geplant und vorbereitet werden. Darunter fallen folgende Punkte:
  - Analyse des möglicherweise aus der Umsetzung des Changes resultierenden Risikos
  - Durchführung notwendiger Tests
  - Definition der für die Umsetzung erforderlichen Schritte
  - Identifizierung und Benachrichtigung der durch den Change betroffenen Parteien
  - Definition eines Fallback-Konzepts
- Freigabe des Notfall-Changes: Im Vorfeld müssen die für die Freigabe von Notfall-Changes autorisierten Personen bestimmt werden.
- Umsetzung des Notfall-Changes: Nach der Freigabe erfolgt die Umsetzung seitens der zuständigen Einheit gemäß den definierten Schritten (siehe Abschnitt „Planung und Vorbereitung des Changes“).
- Zusätzliche Change-Dokumentation: Schritte, die aufgrund der Dringlichkeit des Changes noch nicht erfasst werden konnten, müssen nachträglich dokumentiert werden.

1.2.4 Klassifikation von Changes

Die Klassifikation von Changes erfolgt nach ihrer Komplexität und ihren möglichen Auswirkungen.

Es müssen zumindest folgende Klassen definiert sein:

- Reguläre Changes (gering, mittel, hoch): Der Change ist ein regulärer Change, wenn Änderungen geplant umgesetzt werden sollen. Der Zusatz „gering“, „mittel“ oder „hoch“ weist auf die Komplexität und die möglichen Auswirkungen des Changes hin.
- Notfall-Change: Ein Notfall-Change wird bei einer dringenden Änderung der IT-Systeme erforderlich. Eine solche Dringlichkeit besteht insbesondere wenn ein Schutzziel (Vertraulichkeit, Integrität, Verfügbarkeit, Nachvollziehbarkeit) von einem oder mehreren Geschäftsprozessen verletzt wird und wenn die Umsetzung eines regulären Changes wegen zeitlicher Einschränkungen nicht erfolgen kann. Die Anzahl der Notfall-Changes sollte auf ein Minimum beschränkt werden. Im Falle von Notfall-Changes müssen die Schritte des Notfall-Change-Prozess[8] befolgt werden.

1.3. Anforderungen an das Patch Management

In diesem Zusammenhang wird Patch Management als Change-Modell innerhalb des Change-Management-Prozesses verstanden.

1.3.1 Allgemeine Anforderungen

- Zur Identifizierung verfügbarer Patches müssen ein Prozess und entsprechende Verantwortlichkeiten definiert werden.

[8] Siehe Kapitel 1.2.3

- Dieser Prozess muss sicherstellen, dass jede für ein IT-System zuständige Person über verfügbare Patches in Kenntnis gesetzt wird.
- Für jedes IT-System muss eine Einheit, die für die Implementierung von Patches oder Releases verantwortlich ist, definiert werden.
- Für jedes IT-System muss der Zugriff auf Patches und/oder Releases gewährleistet sein. Bei kommerziellen Produkten kann es der Fall sein, dass der Zugriff auf Patches nur mit einem Wartungsvertrag möglich ist.
- Werden durch die Patches oder Releases Sicherheitslücken geschlossen oder Schwachstellen beseitigt, müssen sie schnellstmöglich implementiert werden. Die Zeitplanung für die Implementierung eines solchen Patches oder Releases geschieht auf Grundlage der Sicherheitsklassifikation des betroffenen Systems durch die für die Implementierung von Patches zuständige Einheit.
- Ein Patch oder Release stellt einen Change an einem IT-System dar und muss daher gemäß dem festgelegten Change-Management-Prozess gehandhabt werden.
- Kritische Patches oder Releases müssen vor ihrer Implementierung getestet werden.
- Kann ein Patch oder Release nicht implementiert werden, ist dies zu dokumentieren und zu begründen. Das Restrisiko muss von der zuständigen Organisationseinheit akzeptiert und dokumentiert werden. Es sollten kompensierende Vorgaben in Betracht gezogen werden, um das erforderliche Sicherheitsniveau einzuhalten.

II. Verantwortlichkeiten

II.I Kapitel 1: Change und Patch Management

Diese Regelung ist von allen Betreibern von IT-Systemen anzuwenden und 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.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(2014)
Change Management	1.2	A.12.1.2	A.10.1.2	12.1

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 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: 06.08.2021

Für die Meldung von Änderungswünschen verwenden Sie bitte das vorgegebene Formular[9].

A.5 Dokumentenhistorie

Version	Name	Org.-Einheit	Datum	Bemerkung
1.0	Andreas Walter	B/FP	07.08.2019	Veröffentlicht

[9] Siehe Anhang A.3.1 Anlage 1 Feedbackformular

B. Spezifische Ausprägungen

B.1 Kapitel 1: Change und Patch Management

B.1.1 Prozessdokumentation „Change Management“ im mynet der AUDI AG unter Geschäftsbereiche -> Beschaffung und IT (B) -> Organisation -> IT (BT) -> IT Service Management ITIL -> Change Management – Hierzu bitte zusätzlich Rücksprache mit IT-Services der AUDI BRUSSELS