Informationssicherheit

Übergreifende Richtlinien und Prozesse

Regelung Nr. 03.01.14

IT Service Continuity Management

Klassifikation: Intern – KSU 2.1

Geltungsbereich: Die Regelungen gelten für die AUDI BRUSSELS

Version 1.1

Inhalt

I. Zweck

Der Zweck dieser Regelung ist die Definition von Anforderungen an die Umsetzung von IT Service Continuity Management (ITSCM) innerhalb der AUDI BRUSSELS.

Im Sinne dieser Regelung bedeutet der Begriff „Informationssicherheit“ IT-Sicherheit als Bestandteil einer ganzheitlichen Informationssicherheit.

1. IT Service Continuity Management (ITSCM)

1.1. Ziele

IT Service Continuity Management ist ein Teil des übergeordneten Business Continuity Management (BCM). ITSCM liefert die Grundlagen für eine kontinuierliche Bereitstellung geschäftskritischer IT Services und hält im Falle einer signifikanten Unterbrechung die Verfügbarkeit der Informationen und Systeme auf einem für das Unternehmen akzeptablen Niveau.

Die ITSCM Ziele sind:

- Geschäftskritische Informationen und Systeme stehen dem Unternehmen mit einem definierten Mindestmaß zur Verfügung.
- Für kritische Services ist eine hinreichende Ausfallsicherheit gegeben.
- Die Effektivität des Kontinuitätsplans wurde anhand von Servicekontinuitätstests verifiziert.
- Die derzeitigen Geschäftsanforderungen sind in einem fortlaufend aktualisierten Kontinuitätsplan abgebildet.
- Interne und externe Parteien wurden im Hinblick auf die ITSCM Richtlinie geschult.

Die Regelung ist ein Instrument, die ITSCM Regeln der IT Organisation zu kommunizieren und damit die IT Governance Ziele und Unternehmenswerte zu unterstützen. Sie liefert gleichzeitig eine Anleitung, was getan werden muss, um bewährte Praktiken zu implementieren.

Zusammenfassend berücksichtigt diese Regelung alle Aspekte des IT Service Continuity Managements. Das übergeordnete BCM ist nicht Bestandteil der Regelung und muss durch den Fach-/Geschäftsbereich berücksichtigt werden.

1.2. Stakeholder

- IT-Sicherheit
- Chief Information Officer (CIO)
- Chief Information Security Officer (CISO)
- Top Management
- IT Compliance Verantwortlicher
- IT Service Operations Manager
- Fach-/Geschäftsbereichsvertreter und Management
- Business Continuity Manager
- ITSCM Prozesseigner und alle verbundenen ITSCM Prozessrollen
- Interne Auditoren (IT Revision)
- Externe Auditoren

- Regulierungsbehörden

Da dieses Dokument alle Prinzipien und Anforderungen innerhalb des ITSCM Prozesses definiert, müssen die oben genannten Stakeholder über die Inhalte und den damit verbundenen Konsequenzen der Regelung aufgeklärt sein.

1.3. ITSCM Prinzipien

1.3.1 Allgemein

Die ITSCM Prinzipien sind Rahmenbedingungen, liefern eine vollständige Liste von „High-Level“ Anforderungen und müssen durch den lokalen ITSCM Prozesseigner berücksichtigt werden, um den ITSCM Prozess effektiv zu steuern. Dies ist eine Voraussetzung zur Etablierung eines nachhaltigen und effektiven ITSCM Prozesses.

Der ITSCM Prozess muss die in Kapitel 1.3.2 bis 1.3.12 aufgeführten Ziele erreichen.

1.3.2 Integration von ITSCM in das übergeordnete Business Continuity Management

Die Fach-/Geschäftsbereiche verantworten das Business Continuity Management (BCM) und somit auch dessen lokale Umsetzung. Da mehr und mehr Geschäftsprozesse durch IT Services unterstützt werden, ist eine Verzahnung des BCM und ITSCM über eine Schnittstelle sicherzustellen. Aus Sicht der IT bedeutet Integration, dass

- in der IT Organisation ein zentraler Ansprechpartner zur Aufnahme von BCM Anforderungen zur Verfügung steht und
- regelmäßige Meetings zwischen Vertretern des ITSCM und BCM zur Verbesserung der Zusammenarbeit und Verfügbarkeit der implementierten IT Services stattfinden.

Dieses gilt unter der Voraussetzung, dass das BCM bereits als Prozess etabliert ist.

1.3.3 Aktuelle ITSCM Richtlinie

Existieren bereits Dokumente zur Kontinuitätspolitik, so sind die Inhalte dieser ISSO-Regelung dort mit abzubilden. Andernfalls kann diese Regelung als Basis für die Erstellung genutzt werden. Das ITSCM Richtliniendokument muss definieren:

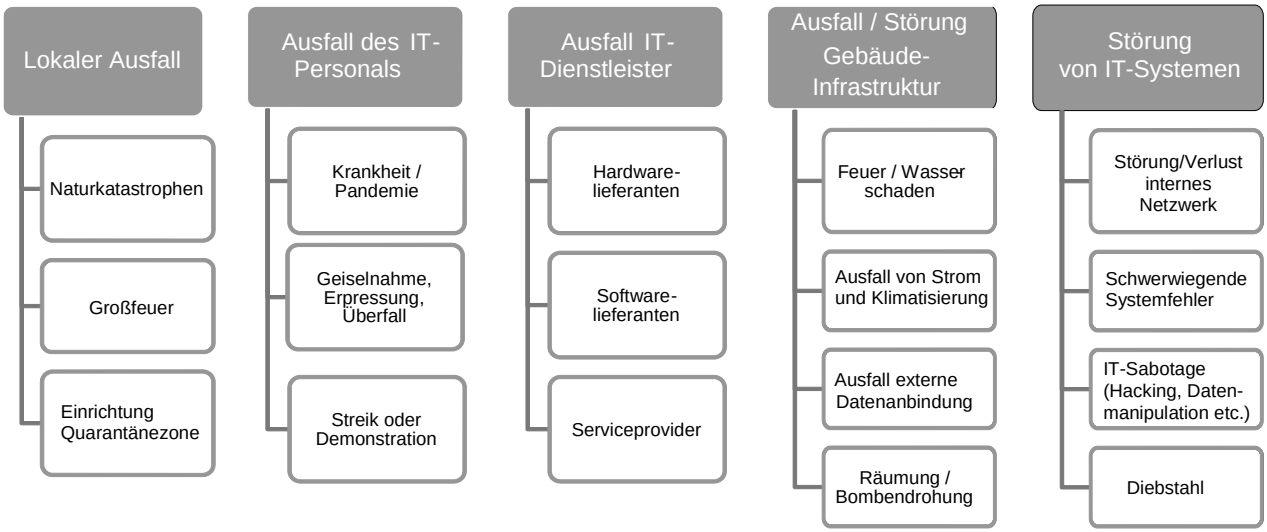
- den Umfang und Geltungsbereich,
- die Szenarien,
- die Verantwortlichkeiten und
- das Rahmenwerk oder Verweis auf den Konzernprozess.

In der Richtlinie soll ebenfalls festgelegt sein, ab welchem Schwellenwert ein kritischer Schaden für die Gesellschaft eintritt.

Die ITSCM Richtlinie stellt zusammen mit weiteren Prozessdokumenten (s. Kap. 1.3.5) die Basis für die Konitinuitätsaktivität dar. Sie muss mit den BCM Aktivitäten abgestimmt sein und muss von Vertretern des BCM mitgetragen werden. Dieses gilt unter der Voraussetzung, dass das BCM bereits als Prozess etabliert ist. Die ITSCM Richtlinie ist mindestens einmal im Jahr zu überprüfen.

Die folgende Abbildung zeigt eine Übersicht möglicher Gründe für IT-Notfallszenarien.

Abbildung 1: Gründe für IT-Notfallszenarien



Es ist mindestens der Ausfall einer Gebäudeinfrastruktur (Rechenzentrum) als Szenario innerhalb des ITSCM zu berücksichtigen. „Scope“ und „Out-of-Scope“ müssen Bestandteil der ITSCM Richtlinie sein.

1.3.4 Aktuelle Business Impact Analysis-IT (BIA-IT) und Business Critical Application List (BCAL)

Die BIA-IT bewertet materielle und nicht-materielle Auswirkungen der kritischen Geschäftsprozesse und unterstützenden IT Anwendungen im Falle eines gravierenden IT-Notfalles über einen bestimmten Zeitverlauf. An Standorten, die geschäftskritische Anwendungen betreiben, muss eine aktuelle Business Impact Analysis-IT (BIA-IT) zur Verfügung stehen, die alle geschäftskritischen Fach-/Geschäftsbereiche sowie die unterstützenden IT Anwendungen umfasst. Die Ergebnisse müssen vom Leiter der Fach-/Geschäftsbereiche bestätigt werden.

Es wird empfohlen, lokale Koordinatoren in den Fach-/Geschäftsbereichen oder in der IT zu etablieren, die die Durchführung der BIA-IT koordinieren. Als Mindestanforderung müssen für alle kritischen IT Anwendungen die folgenden Parameter durch den Fach-/Geschäftsbereich ermittelt und durch die ITSC-Verantwortlichen in der sogenannten „Business Critical Application List (BCAL)“ dokumentiert werden:

- Eindeutige Bezeichnung/Kennung (planningIT ICT OBJECT ID)[1],
- Anwendungskurzname,
- Betrieben durch (Beispiel: RZ, Verteilt über mehrere RZ, Externer Service Provider),
- Werte zu finanziellen Schäden, Reputationsschäden und gesetzlichen Auswirkungen, basierend auf den Werten der globalen Governance, Risk und Compliance (GRC) Organisation,
- Recovery Time Objective (RTO - maximale Wiederanlaufzeit) und
- Recovery Point Objective (RPO - maximaler Datenverlust).

[1] Die eindeutige Bezeichnung und Anwendungsname lt. Systemverzeichnis (planningIT).

Die BIA-IT Werte müssen spätestens nach 2 Jahren unter Einbezug des Fachbereichs geprüft und bei gravierenden Änderungen durch das lokale Fach-/Geschäftsbereichs Management Gremium bestätigt werden.

Vorlagen für die BIA-IT und die BCAL können bei den lokalen Prozessverantwortlichen angefordert werden. Außerdem werden Vorlagen für die Nutzung im Konzern an einer zentralen Stelle bereitgestellt (s. Anhang A.5.1).

1.3.5 Aktuelle ITSCM Dokumente

Im Falle eines IT-Notfalls ist es sehr wichtig, dass die IT Organisation in der Lage ist, einem strukturierten und gesteuerten Wiederanlaufprozess zu folgen. Als Voraussetzung müssen die folgenden ITSCM Dokumente verfügbar und mit der lokalen ITSCM Richtlinie abgestimmt sein:

- 1 x IT-Notfallhandbuch (IT-NHB),
- Disaster / Application Recovery Plans (DRP/ARP) für alle geschäftskritischen Anwendungen und der verbundenen Basis-Infrastrukturservices,
- ITSCM Prozesshandbuch (siehe ebenso Kapitel1.3.6).

Diese Dokumente müssen aktuell sein und müssen kontinuierlich verbessert werden. Die Dokumente sind mindestens einmal im Jahr zu überprüfen. Aktualisierungen müssen an alle relevanten Stakeholder kommuniziert werden. Es muss sichergestellt sein, dass die aktuelle Dokumentation für alle Stakeholder verfügbar ist[2].

Das IT-Notfallhandbuch ist insbesondere für IT betreibende Standorte oder Lokationen, die in einem starken Maß von IT-Systemen abhängig sind, erforderlich und muss die folgenden Themen beinhalten:

- Umfang der IT-Notfallszenarien, die dieses Handbuch berücksichtigt,
- Definition IT-Notfall / Krisen Management, seiner Mitglieder und Stellvertreter,
- formelles Alarmierungs- und Eskalationsverfahren,
- Kommunikationsplan für die interne IT Organisation und externe Stakeholder,
- Wiederanlaufreihenfolge für IT Infrastruktur und IT Anwendungen,
- formelles De-Eskalationsverfahren und
- die für die Alarmierung und organisierte, strukturierte Kommunikation innerhalb des IT-Notfallbewältigungsprozesses notwendigen Kontaktinformationen.

Alle DRP/ARPs müssen die folgenden Themen beinhalten:

- Definition der Wiederanlaufparameter RTO/RPO basierend auf den Ergebnissen der BIA-IT[3] (siehe Kapitel 1.3.4) und unter Berücksichtigung von SLA's oder vergleichbaren Vereinbarungen,
- kurze Beschreibung der Anwendung / des Services,
- Beschreibung[4] der Systemarchitektur der Anwendung / des Services, z. B.

[2] Siehe Kapitel 1.3.11

[3] Neben der BIA wird bei Audi zusätzlich eine Widerstandfähigkeitsanalyse durchgeführt

[4] Detaillierte Konfigurationsinformation (Name lpar, Liste der virtuellen Disks, Konfigurationsdateien) können auch in separaten Dokumenten und speziellen Systemen gespeichert werden. Es muss jedoch sichergestellt sein, dass die Informationen im Notfall vorhanden sind.

  - Physischer Standort der Systemkomponenten (Rack-Zeile, Rack-Nummer, Rack-Position, etc…),
  - Servername, LPAR Name (Logische Partition),
  - Databankname, Datenbankinstanz,
  - Middleware-Instanz (z. B. WebSphere, MQSeries, IMS, CICS),
  - Schnittstellen zu anderen Anwendungen oder Systemen (in grafischem Format dargestellt) inklusive einer Liste der unterstützenden IT Services oder anderer nicht-IT Voraussetzungen, auf denen der Service beruht und die zuerst wiederhergestellt sein müssen,
  - Physischer Standort der Datensicherung oder von Installationsmedien und
  - Servicevertragsnummern.

- Kontaktinformationen inklusive Stellvertreter[5]. Diese Kontaktliste muss die folgenden Informationen enthalten:
  - IT-Notfall- / Krisenteam,
  - OE Leiter der entsprechenden Anwendung / des Services,
  - Service Manager oder Service Owner (falls verfügbar / existent),
  - Koordinator des Wiederanlaufteams inklusive Stellvertreter,
  - Wiederanlaufteam (kann intern oder durch externe Lieferanten besetzt sein),
  - Process Integration Officer (PIO), falls für den Wiederanlauf der Anwendung / des Services notwendig,
  - Fach-/Geschäftsbereich, falls für den Wiederanlauf der Anwendung / des Services notwendig und
  - Zusätzliche, unterstützende Teams, falls für den Wiederanlauf der Anwendung / des Services notwendig (z.B. Betrieb, Server Administrator, Datenbank Administrator).
- Alarmierungsplan: Informationen über die Alarmierung und Aktivierung der Wiederanlaufteams und
- Wiederanlaufreihenfolge der Anwendungen / Services: Definition aller Voraussetzungen, Aktionspläne, Prüfpunkte und Aufgaben, welche für den Wiederanlauf der Anwendung / des Services notwendig sind oder ausgeführt werden müssen.
- Zusätzliche, optionale Anforderungen sind:
  - Risikoliste: Referenz zu Dokumenten, die Risiken und/oder andere Probleme bzgl. der Funktionsweise des DRP/ARP beinhalten,
  - Definition kritischer Objekte: Beschreibung der Komponenten, die ausfallen können oder dürfen und Beschreibung der dazugehörigen Aufgaben oder Komponenten, die diesen Ausfall abfangen und

[5] Kontaktinformationen können auch in separaten Dokumenten gespeichert werden. Es muss jedoch sichergestellt sein, dass die Informationen im Notfall vorhanden sind.

- identifizierte “Single Point of Failures (SpoF)”: SpoF sind Komponenten, die nicht redundant verfügbar sind und deren Ausfall gravierende Auswirkungen auf die Wiederanlaufzeit (RTO) haben.

Anweisungen und Vorlagen stehen zur Verfügung und können beim Prozess Ansprechpartner angefragt werden[6].

1.3.6 Etablierung eines ITSCM Prozesses und entsprechender Rollen

Alle ITSCM Aktivitäten müssen durch den ITSCM Prozess gesteuert werden. Der Prozess selbst beinhaltet drei Kernprozesse:

- IT-Notfallbewältigung
- IT-Notfallvorsorge
- Kontinuierliche Verbesserung

Alle drei Prozesse müssen im ITSCM Prozesshandbuch beschrieben sein. Die IT-Notfallbewältigung muss ebenfalls im IT-Notfallhandbuch (IT-NHB) beschrieben sein, jedoch müssen dort nur die für die IT-Notfallbewältigung notwendigen Informationen aufgeführt werden. Allgemeine Informationen müssen im ITSCM Prozesshandbuch enthalten sein.

Die IT-Notfallbewältigung muss mit dem Incident Management abgestimmt sein. Die Schnittstelle zwischen dem Incident Management und ITSCM muss Bestandteil des IT-NHB oder ITSCM Prozesshandbuchs sein.

Der ITSCM-Verantwortliche (Prozess-Manager) der Gesellschaft ist dem Prozessverantwortlichen der AUDI BRUSSELS bekannt zu machen (Kontaktinformation siehe Anhang A5.1)

Die ITSCM Unterprozesse müssen die folgenden Anforderungen erfüllen:

- Die Prozesse müssen dokumentiert sein und es muss festgelegt sein, wer für Aktualisierung und Freigabe verantwortlich ist.
- Die Prozessdokumentation muss einmal im Jahr überprüft werden oder wenn sich Prozesse geändert haben,
- als Mindestanforderung muss der Prozess einen Eigner (Owner) sowie einen Prozess Manager haben und die Verknüpfung zwischen Prozessaktivitäten und Rollen muss durch eine RACI-Matrix dokumentiert sein (R=Responsible, A=Accountable, C=Consulted, I=Informed),
- der IT-Notfallbewältigungsprozess muss ein IT-Notfall- / Krisenteam (inklusive einem Leiter) und dazugehörige Wiederanlaufteams (DRP/ARP Koordinatoren) beinhalten,
- die Rollen müssen individuellen Personen inklusive Stellvertretern zugewiesen sein,
- dem Prozess sind genügend Ressourcen zu allokieren (als Mindestanforderung ist eine Gewaltenteilung zu realisieren, so dass die Mitglieder des IT-Notfallteams/Krisenstabs nicht gleichzeitig Bestandteil der technischen Wiederanlaufteams sind),

[6] Siehe Anhang A.5.1

- es muss ein regelmäßiges Berichtswesen über den ITSCM Reifegrad und der dazugehörigen drei Kernprozesse inklusive einer Übersicht der Wiederanlauftests etabliert sein und
- die Schnittstellen zu anderen Prozessen (z.B. Incident-, Change- und IT Risiko Management) müssen beschrieben sein.

1.3.7 Regelmäßige ITSCM Tests und Übungen

IT-NHB und DRP/ARP müssen regelmäßig getestet und geübt werden (mindestens einmal im Jahr), um sicherzustellen, dass die IT Systeme effektiv wiederhergestellt werden können. Die Tests müssen geplant (Testplan) und dokumentiert (Testprotokoll) werden. Die Ergebnisse müssen an den ITSC Prozess Manager zur Bewertung berichtet werden und es muss ein Verbesserungsplan entsprechend der Testergebnisse implementiert werden.

Als Übungsarten kommen Plan-Review-Tests, Kommunikations- und Alarmierungsübungen sowie Funktionstests in Betracht. Dabei sind die Personen einzubinden, die im Notfall einen Wiederanlauf durchführen müssen (z.B. Recovery Teams, Krisenstab). Teststrategien und alle entsprechenden Testaktivitäten müssen auf den IT-Notfallszenarien basieren, die das ITSCM berücksichtigt[7] (siehe auch Kapitel 1.3.9). Zum Beispiel: Wenn die RTO nur durch eine Systemredundanz zu erreichen ist, dann ist diese Redundanz zu testen.

Die Effektivität des IT-NHB muss unter Verwendung realer Szenarien getestet und geübt werden.

Umfang der Tests/Übungen:

- Schätzen oder messen der realen/effektiven RTO,
- Identifizieren der Schwachstellen in der Wiederanlaufsequenz und
- Identifizieren der Schwachstellen in der Kontaktliste (z.B. Verantwortlichkeiten).

Alle Test- und Übungsergebnisse müssen dem lokalen ITSCM Manager zur Verfügung gestellt werden.

1.3.8 Integration des ITSCM in den Change Management Prozess

Das Change Management muss die Auswirkungen einer Veränderung (Change) auf ITSCM und aller dazugehörigen Aspekte bewerten. Der Fokus liegt dabei auf

- der Aktualisierung des IT-NHB und der DRP/ARPs und
- dem Test der technischen Funktionalität zur Erreichung der Werte für RPO und RTO (z.B. Failover- oder Redundanztests).

Die Beschreibung der Integration von ITSCM und Change Management muss sowohl Bestandteil des ITSCM Prozesshandbuchs als auch der Change Management Dokumentation sein.

1.3.9 Integration des ITSCM in den IT Risiko Management Prozess

Die bei der DRP-Erstellung oder während Disaster Recovery Tests identifizierten, inakzeptablen Schwachstellen/Risiken werden vom ITSC Manager an die entsprechenden Ansprechpartner im IT Risiko Management übergeben und dort bearbeitet. Im Rahmen des

[7] Der Umfang der Wiederanlaufszenarien kann variieren: Vom Test einer einzelnen Anwendung über integrierte Testszenarien bis hin zu einem Ende-zu-Ende Test inklusive Lieferantentests.

kontinuierlichen Verbesserungsprozesses überprüft der ITSC Manager mindestens einmal jährlich den aktuellen Status der identifizierten Risiken.

Einfache, insbesondere lokale und technische Schwachstellen sollten an das Problem Management übergeben werden. Die Einbeziehung des Risiko Managements wäre in diesen Fällen nicht effizient.

Applikationen, welche bei der die Verfügbarkeit als „sehr hoch“ eingestuft sind, haben die Anforderungen aus A 1.2 (ITSCM_Requirements) zu erfüllen. Abweichungen werden im Information-Security-Risiko-Management behandelt.

1.3.10 Ausgelagerte Datensicherungsmedien

Alle kritischen Datensicherungsmedien müssen über ein Standortkonzept abgesichert sein. Der Auslagerungsstandort muss sich außerhalb der Reichweite der betrachteten IT-Notfallszenarios befinden.

Der Wiederanlauf auf Basis der ausgelagerten Datensicherung muss mindestens einmal im Jahr getestet werden. Dabei ist die vollständige Zeit, die für den Wiederanlauf auf Basis ausgelagerter Datensicherung notwendig ist (z.B. Transportzeit, etc.), zu dokumentieren.

1.3.11 Verfügbarkeit und Verteilung der ITSCM Dokumente

Eine definierte und kontrollierte Dokumentenverteilungsstrategie muss implementiert sein. So muss sichergestellt werden, dass alle ITSCM Pläne und verbundenen Dokumente wie IT-NHB, DRP/ARP sowie Betriebshandbücher in einer vernünftigen und sicheren Art und Weise verteilt werden und somit den autorisierten und interessierten Parteien zur Verfügung stehen, wann und wo sie die Dokumente benötigen. Die Pläne müssen unter allen definierten IT-Notfallszenarien zugänglich sein.

Die Verfügbarkeits- und Verteilungsstrategie muss in den ITSCM Dokumenten beschrieben sein und die Effektivität dieser Strategie muss mindestens einmal im Jahr getestet werden (siehe Kapitel 0).

1.3.12 Lieferantenvereinbarungen für IT-Notfälle

Falls externe Lieferanten innerhalb geschäftskritischer Prozesse eingebunden sind, müssen diese Service Provider im ITSCM Prozess berücksichtigt werden. Ihre Mitwirkungspflichten während der IT-Notfallbewältigung oder IT-Notfalltest müssen in formellen Service Level Agreements oder Absicherungsverträgen geregelt sein.

II. Verantwortlichkeiten

II.I Kapitel 1: IT Service Continuity Management

Diese Regelung muss von allen ITSCM Process Ownern, ITSCM Prozess Managern und zugewiesenen Rollen innerhalb des ITSCM Prozesses eingehalten werden.

Abweichungen von dieser Regelung, die das Sicherheitsniveau reduzieren, sind nur zeitlich begrenzt nach Rücksprache mit der IT-Sicherheit erlaubt.

Anhang

A. Allgemeines

A.1 Mitgeltende Dokumente

A.1.1 Informationssicherheit Regelung Nr. 03.01.09 Ausnahmeprozess

A.1.2 ITSCM_Requirements

A.2 Anlagen

A.2.1 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.3 Quellen und Referenzen

A.3.1 Referenz zu Standards

Die folgende Tabelle verdeutlicht die Referenzen zu ISO/IEC 27001:13 und VDA.

Thema	**Kapitel**	**ISO 27001:2013**	**VDA (Information Security Assessment)**
Planen der Informationssicherheitskontinuität	1.3.4, 1.3.10	A.17.1.1	17.1
Implementierung der Informationssicherheitskontinuität	1.3.1 - 1.3.8, 1.3.11- 1.3.12	A.17.1.2	17.1

Prüfen, durchsehen und bewerten der Informationssicherheitskontinuität	1.3.7, 1.3.8	A.17.1.3	17.1
Verfügbarkeit von Informationsverarbeitenden Einrichtungen	1.1, 1.3.3	A.17.2.1	17.1

A.3.2 ITIL V3

A.3.3 ISO 20000

A.3.4 COBIT®5, DSS04 Managen der Kontinuität

A.3.5 Bundesamt für Sicherheit in der Informationstechnologie, BSI Standard 100-4

A.4 Abkürzungen und Definitionen

Begriff / Abkürzung	Definition
Application Recovery Plan (ARP)	Ein Dokument das detaillierte Arbeitsanweisungen zum Wiederanlauf einer einzelnen Anwendung (Application) zusammenfasst. Die Reihenfolge, in der einzelne ARPs zueinander stehen wird entweder in DRPs oder IT-Notfallhandbüchern dokumentiert.
Business Continuity Management (BCM)	Der Business-Prozess, der für den Umgang mit operativen Risiken verantwortlich ist, die zu schwerwiegenden Auswirkungen auf das Business führen können. Das BCM sichert die Interessen der wichtigsten Stakeholder, sowie das Ansehen, die Marke und die wertschöpfenden Aktivitäten des Business. Für den Fall einer Unterbrechung der Geschäftsabläufe werden im BCM-Prozess die Risiken auf ein akzeptables Maß reduziert und eine Planung der Wiederherstellung von Business-Prozessen vorgenommen. Ein Bestandteil des BCM ist das IT Service Continuity Management zur Absicherung des Unternehmens gegen IT-Notfälle.
Business Impact Analyse-IT (BIA-IT)	Die BIA-IT ist die Aktivität im IT Service Continuity Management, die die Vital Business Functions und deren Abhängigkeiten identifiziert. Diese Abhängigkeiten können zwischen Suppliern, Mitarbeitern, anderen Business-Prozessen, IT Services etc. bestehen. Die BIA-IT definiert die Wiederherstellungsanforderungen für IT Services. Zu diesen Anforderungen gehören die maximale Wiederherstellungszeit nach einem Ausfall, der tolerierte Datenverlust aufgrund von Ausfällen und die mindestens erforderlichen Service Level Ziele für die jeweiligen IT Services. Des Weiteren beschreibt die BIA-IT die Auswirkungen eines längerfristigen IT-Ausfalls bei Eintritt eines (IT-) Notfalls.
Disaster Recovery Plan (DRP)	Anwendungen, die nur im Zusammenhang mit anderen Anwendungen konsistent wiederhergestellt werden können werden als Anwendungsverbund oder Anwendungscluster bezeichnet. Die hierzu erforderliche Wiederanlaufdokumentation wird in einem DRP

	zusammengefasst. Der DRP beinhaltet alle Informationen zum Wiederanlauf der einzelnen Anwendungen bzw. verweist auf die entsprechenden ARPs (Anwendungs Recovery Pläne) und dokumentiert die Reihenfolge in der die ARPs ausgeführt werden müssen um den Anwendungsverbund wiederherzustellen.
IT-Notfallhandbuch (IT-NHB)	Das IT-Notfallhandbuch beinhaltet alle Informationen, die während und für die Notfall- und Krisenbewältigung benötigt werden. Es umfasst somit alle Notfallpläne wie den Krisenkommunikationsplan, den Krisenstabsleitfaden, die Wiederanlauf- und Wiederherstellungspläne.
IT Service Continuity Management (ITSCM)	Der Prozess, der für die Erfassung und Behandlung von Risiken verantwortlich ist, die zu schwerwiegenden Auswirkungen auf IT Services führen können. Das ITSCM stellt sicher, dass der IT Service Provider stets ein Mindestmaß der vereinbarten Service Levels bereitstellen kann, indem die Risiken auf ein akzeptables Maß reduziert werden und eine Wiederherstellungsplanung für IT Services erfolgt. Das ITSCM soll so konzipiert sein, dass es das Business Continuity Management unterstützt.
Recovery Point Objective (RPO)	Die maximale Menge an Daten, die bei der Wiederherstellung eines Service nach einer Unterbrechung verloren gehen darf. Der RPO wird als Zeitspanne vor dem Ausfall ausgedrückt. Ein RPO von einem Tag kann beispielsweise durch tägliche Backups unterstützt werden, so dass maximal Datenmengen aus dem Zeitraum von 24 Stunden verloren gehen können. RPOs sollten für jeden IT Service verhandelt, vereinbart, dokumentiert und anschließend als Anforderungen für das Service Design und IT Service Continuity Pläne verwendet werden.
Recovery Time Objective (RTO)	Die Wiederanlaufzeit eines Prozesses oder der benötigten Ressourcen. Die maximale Zeit für den Wiederanlauf muss kleiner als die maximal tolerierbare Ausfallzeit sein.

A.5 Ansprechpartner

A.5.1 Globaler ITSCM Prozess Manager: IT

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[8].

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 Kapitel 1.3.9

[8] Siehe Anhang A.2.1 Anlage 1 Feedbackformular

B. Spezifische Ausprägungen

B.1 Kapitel 1: IT Service Continuity Management (ITSCM)