Arbeitsrichtlinie Datensicherung

VAV Versicherungs-Aktiengesellschaft

Klassifikation: Intern
Version 21.0

VAV VERSICHERUNGEN

Dokumenteneigenschaften

Titel	Arbeitsrichtlinie Datensicherung
Version	21.0
Geltungsbereich	Siehe Geltungsbereich Richtlinie Informationssicherheit
Erstmalige Freigabe	20.11.2019
Verabschiedet durch	Daniel Fürdauer (Informationssicherheitsbeauftragter)
Klassifikation	Intern
Verantwortlicher Verantwortliche Abteilung	Daniel Fürdauer Datenschutz und Informationssicherheit
Fachlicher Ansprechpartner	Daniel Fürdauer (daniel.fuerdauer@vav.at)
Letztes Review	November 2021

Dokumentenhistorie

Version	Datum	Beschreibung der Änderung	Ersteller
19.0	20.11.2019	Ersterstellung in Anlehnung an die entsprechende Arbeitsrichtlinie der VHV in der Version 19.0.	Daniel Fürdauer
20.0	04.12.2020	In Anlehnung an die entsprechende Arbeitsrichtlinie der VHV in der Version 20.0: • Klare Abgrenzung von System, Konfiguration und Daten in Kapitel 5.1 • Erweiterung der möglichen zugelassenen Quellen zur Wiederherstellung von Betriebssystemen und Standardsoftware in Kapitel 5.3.	Daniel Fürdauer
21.0	22.11.2021	Review ohne Änderungen	Daniel Fürdauer

Hinweis zur Schreibweise

Die verwendete männliche Sprachform dient der leichteren Lesbarkeit und meint immer alle Geschlechter (m/w/d). Die verkürzte Sprachform hat nur redaktionelle Gründe und beinhaltet keine Wertung.

INHALTSVERZEICHNIS

1. ZIELSETZUNG

Ziel dieser Richtlinie zur Datensicherung ist es, die Aufbewahrungs- und Schutzanforderungen in Bezug auf Datensicherungen (Backups) festzulegen, um einen Verlust von Daten zu verhindern. Eine Datensicherung soll gewährleisten, dass mit dem gesicherten Datenbestand der IT-Betrieb nach einem Ausfall oder Fehlerfall kurzfristig wiederhergestellt werden kann.

2. ABGRENZUNG

Die Vorgaben gelten für die Datensicherung aller produktiven IT-Systeme sowie der damit zusammenhängenden Anwendungen, Hardwarekomponenten und Konfigurationseinstellungen. Diese Richtlinie gilt nicht für Entwicklungs- oder Testsysteme, sofern sie keine produktiven Daten enthalten. Nicht Bestandteil dieser Richtlinie ist die Archivierung von Daten, welche durch gesetzliche und / oder regulatorische Anforderungen eine Aufbewahrungsdauer / Archivierung fordern. Diese konkreten Aufbewahrungsfristen sind maßgeblich umzusetzen. Gleiches gilt, wenn Betriebsvereinbarungen konkrete Aufbewahrungsfristen fordern.

3. GRUNDSÄTZLICHE ANFORDERUNGEN

Zur Festlegung der Datensicherungsanforderungen müssen die zu sichernden Daten von IT-Systemen spezifiziert werden, die für den Betrieb erforderlich sind. Dazu gehören Systemdaten (z.B. Initialisierungsdateien, Konfigurationsdaten), Protokolldaten (z.B. Syslog-Daten, Log-Daten), Anwendungsdaten (Applikationen) und Rohdaten.
Der Umfang und die Häufigkeit der Datensicherungen müssen den geschäftlichen Anforderungen, den internen Sicherheitsanforderungen bezüglich des Schutzbedarfs und der Wichtigkeit der Information für die Fortführung der Betriebstätigkeit entsprechen. In Fällen, in denen ein hoher Schutzbedarf besteht, müssen die Datensicherungen mittels Verschlüsselung geschützt werden. Hierbei sind Verschlüsselungsverfahren nach dem Stand der Technik einzusetzen.

Ausnahmen unterliegen der Risikobewertung durch die Stabstelle Datenschutz und Informationssicherheit und müssen sowohl zentral als auch im jeweiligen Betriebshandbuch durch den Produktverantwortlichen dokumentiert werden. Im Falle von Restrisiken ist eine Risikoübernahme durch den Risikoverantwortlichen entsprechend der in der Konzernrichtlinie Informationssicherheit definierten Verfahren erforderlich.
Die Vorgaben für die Verfahren zur Datensicherung sind schriftlich in einem Datensicherungskonzept zu hinterlegen. In diesem sind ebenfalls Rollen und Berechtigungen zu regeln. Außerdem muss bei Konfigurationsänderungen gewährleistet sein, dass diese durch organisatorische und / oder technische Maßnahmen gesteuert werden. Änderungen an Konfigurationen sind nachvollziehbar zu dokumentieren.

Für ortsveränderliche Backup-Datenträger müssen geeignete Aufbewahrungsorte (geschützt vor dem Zugriff unbefugter Dritter) festgelegt werden, welche sich in ausreichender Entfernung zu den Originalspeicherorten befinden. Ebenfalls sind wirksame Maßnahmen zu ergreifen, um die Datenträger vor umwelt- und sonstigen äußeren Einflüssen zu schützen. Defekte oder nicht mehr benötigte Backup-Datenträger müssen nach Ablauf der Vorhaltezeit von einem zertifizierten Dienstleister vernichtet oder unbrauchbar gemacht werden, entsprechend der Arbeitsrichtlinie Entsorgung von Datenträgern.
Das Datensicherungssystem muss gesammelte Daten verschiedener Quellensysteme logisch voneinander trennen und speichern.
Für Datensicherungssysteme muss eine Synchronisation der Systemzeit mit einer vertrauenswürdigen Quelle erfolgen, um im Bedarfsfall zeitliche korrekte Daten wieder herstellen zu können.
Im Rahmen der Betriebsabläufe müssen die Durchführung von Datensicherungen überwacht und Maßnahmen bei fehlgeschlagenen geplanten Datensicherungen festlegt werden, um die Vollständigkeit der Backups nach der Datensicherungsrichtlinie zu gewährleisten.
Datensicherungen dürfen nur maximal 25 Stunden auf lokalen IT-Systemen vorgehalten und müssen auf zentrale Datensicherungsmedien übertragen und gespeichert werden.
Datensicherungen müssen bei der Sicherung, Übertragung und Speicherung vor unberechtigter Einsichtnahme und Veränderung geschützt werden.
Protokolle der Datensicherungssysteme müssen auf dem zentralen Protokollierungs-System gespeichert werden. Die Protokolle müssen entsprechend der Vorgaben der Arbeitsrichtlinie Protokollierung und Überwachung aufbewahrt werden. Ausnahmen müssen durch die Stabstelle Datenschutz und Informationssicherheit bewertet und durch den Produktverantwortlichen dokumentiert werden.

Für die Wiederherstellung eines Datenbestandes oder von Teilen (einzelne Dateien oder Datensätze) muss regelmäßig geprüft werden, ob mit den vorhandenen Datensicherungen ein solches Vorhaben durchgeführt werden kann. Diese Wiederherstellung darf die Verfügbarkeit der IT-Systeme, Anwendungen oder die Netze nicht gefährden.

4. AUSWAHL DES DATENSICHERUNGSVERFAHRENS

Für alle IT-Systeme muss ein Datensicherungsverfahren etabliert werden. Dieses Datensicherungsverfahren muss auf allen IT-Systemen anwendbar sein, mit dem Ziel, Datensicherungen für die Wiederherstellung der IT-Systeme vorzuhalten.
Damit alle Richtlinien und Anforderungen an das Backup-Management erfüllt werden, muss auf den jeweiligen IT-Systemen Backup-Software eingesetzt und herstellerspezifische Sicherungssoftware angewendet werden.
Ein Backup-Management zur Verwaltung und Steuerung der Datensicherung muss entwickelt werden, damit die Übertragung und Speicherung der Backup-Sicherungen auf zentralen Datensicherungssystemen erfolgt.

5. DATENSICHERUNGSPLAN

Die Verfahrensweise einer Datensicherung wird von einer Vielzahl von Einflussfaktoren bestimmt. In den nachfolgenden Kapiteln wird auf diese Einflussfaktoren eingegangen und es werden Anforderungen an den Datensicherungsplan abgeleitet.
Konkrete Ausprägungen bezüglich der Einflussfaktoren Datenvolumen, Änderungsvolumen, Vorhaltezeiten, Fristen sind zu dokumentieren.

5.1. Datengruppen

Für die Wiederherstellung der Quellsysteme ist grundsätzlich sicherzustellen, dass die Ausgestaltung der Backups so zu erfolgen hat, das folgende Datengruppen im Bedarfsfall einzeln wiederherzustellen sind:

- Systemdaten
- Konfigurationsdaten
- Nutzdaten / Rohdaten

Im begründeten Einzelfall kann von dieser Trennung abgewichen werden, wenn beispielsweise die Trennung aus technologischer Sicht keinen Mehrwert bringt. Die Begründung ist vom Gruppenleiter zu dokumentieren und mit der Stabstelle Datenschutz und Informationssicherheit abzustimmen.
Ein Sonderfall ergibt sich bei der Sicherung von virtuellen Maschinen. Da hier die Datensicherung mittels Snapshot-Technik erfolgen kann, ist eine Differenzierung der Datengruppen nicht möglich.

5.1.1. Systemdaten

Die Datengruppe der Systemdaten sollte eine Vollsicherung mit Betriebssystemsoftware und Anwendungssoftware umfassen. Diese Art der Vollsicherung kann eine zeitnahe Wiederherstellung sicherstellen. Diese Gruppe von Systemdaten kann u. a. Snapshots und Backups von ganzen Systemen enthalten.

5.1.2. Konfigurationsdaten

Die Datengruppe Konfigurationsdaten muss spezifische Dateien und Konfigurationsparameter enthalten, die für eine Wiederherstellung der IT-Systeme und Anwendungen erforderlich sind. Konfigurationsdaten können digital, im Rahmen von Konfigurationssicherungen oder in Form von Dokumentationen vorgehalten werden. Zielsetzung ist ein Wiederaufbau der benötigten Systemkonfiguration im Fehlerfall.

5.1.3. Nutzdaten / Rohdaten

Die Datengruppe Nutzdaten / Rohdaten muss spezifische Daten einzelner Anwendungen enthalten, die im Fehlerfall auch auf neu aufgesetzte Quellsysteme wieder eingespielt werden können. Diese Gruppe von Nutzdaten / Rohdaten kann u. a. Filesysteme oder Datenbanken enthalten.

5.2. Verfügbarkeitsanforderungen an die Daten

Mit einer Datensicherung muss eine Wiederherstellung der IT-Systeme und Softwarekomponenten aus dem Datensicherungsbestand möglich sein. Dabei muss gewährleistet sein, dass mit den Datensicherungen die Wiederherstellung der IT-Systeme, Betriebssysteme und Anwendungen auch in Teilen erfolgen kann.
Durch Redundanzmechanismen für IT-Systeme in der VAV muss gewährleistet sein, dass die Betriebsfähigkeit weitergeführt werden kann, ohne auf Datensicherungsbestände zurückgreifen zu müssen. Die Wiederherstellungszeit und der maximal tolerierbare Datenverlust (engl. RPO: Recovery Point Objective) von IT-Systemen ist zu definieren.
Die IT-Systeme aller Standorte müssen durch Backupsysteme gesichert werden.
Die technologische Nutzbarkeit und Vorhaltung entsprechender Hardware muss bei langfristigen Backups sichergestellt werden.

5.3. Wiederherstellung von Betriebssystemen & Standardanwendungen ohne Systemsicherung

Bei der Wiederherstellung von Betriebssystemen und Standardanwendungen kann auf verifizierte Quellen der Hersteller zurückgegriffen werden, sofern keine Systemsicherung vorliegt. Die Wiederherstellung der VAV spezifischen Konfiguration der Betriebssystemparameter muss aus dem Datensicherungsbestand oder manuell mit Hilfe der Systemdokumentation erfolgen. Für Systeme, die durch Lieferanten bereitgestellt werden, sind die Vorgaben zur Datensicherung über entsprechende Vereinbarungen (SLA) zu definieren und deren Einhaltung ist regelmäßig zu kontrollieren.
Bei IT-Systemen mit spezifischem IOS (Internal Operation System) oder integrierter Firmware OS (Operation System (Appliance)) wird die Betriebssystemsoftware nicht gesichert. Bei diesen IT-Systemen liefert der Hersteller die aktuelle IOS / OS Betriebssystemsoftware.
Bei IOS / OS Betriebssystemen muss die Wiederherstellung der VAV spezifischen Konfiguration der Betriebssystemparameter aus dem Datensicherungsbestand oder manuell mit Hilfe der Systemdokumentation erfolgen.

5.4. Datenvolumen / Änderungsvolumen der Datensicherung

In Abhängigkeit der eingesetzten Backup-Software, Backupverfahren und Komprimierung ist eine Abschätzung des Datenvolumens der Datensicherung erst nach der Installation der IT-Systeme möglich.
Das Datenvolumen der Datensicherung für Betriebssysteme, Konfigurationsdaten, Anwendungen und Anwendungsdaten sollte nach der Erstkonfiguration und Inbetriebnahme des IT-System erfasst werden.
Das Änderungsvolumen der Datensicherung wird bestimmt durch das Sicherungsverfahren, das Sicherungsintervall und durch Anwendungen, die unmittelbar Daten erzeugen und erheben.

5.5. Änderungshäufigkeit- / Änderungszeitpunkt- / Häufigkeit der Datensicherung

Es ist zu spezifizieren, welche IT-Systeme täglich gesichert werden müssen.
Die Sicherung des Datenbestands für Betriebssysteme, Anwendungen und Konfigurationen der IT-Systeme muss einmal täglich gestartet werden.
Die Sicherung sollte außerhalb der Kernarbeitszeit, vorrangig in den Nacht- und Morgenstunden erfolgen, um Änderungen im täglichen Betrieb vollständig erfassen zu können.
Vor grundlegenden Änderungen und Anpassungen in den Anwendungen und vor Wartungsarbeiten müssen zusätzliche Datensicherungen durchgeführt werden. Diese müssen zusätzlich zu den regelmäßigen Sicherungsintervallen auf den Datensicherungssystemen gespeichert werden.
Rohdaten, die zur Wiederherstellung von Anwendungen erforderlich sind (DBMS-Exporte / Sicherungen von Anwendungsparameter, Konfigurationsdateien) müssen entsprechend der Vorgaben aus dem BCM, ITSCM, Notfallplänen und Wiederanlaufzeiten gesichert werden.

5.6. Transportmodalitäten

Bei der Durchführung einer Datensicherung werden Daten über ein Netz oder eine Leitung übertragen oder Datenträger zum Datenträgerarchiv transportiert.
Bei der Auswahl des Datenübertragungsmediums beziehungsweise des Datenträger-Transportweges sind die Verfügbarkeitsanforderungen zu berücksichtigen. Wenn zur Datenrekonstruierung die Daten über ein Netz übertragen werden, muss bei der Auswahl der Übertragungskapazität des Netzes das Datenvolumen beachtet werden. Es ist zum Zeitpunkt der Datensicherung eine ausreichende Datenübertragungskapazität sicherzustellen.
Der physische Versand oder Transport von Datenträgern muss in der Weise erfolgen, dass eine Beschädigung der Datenträger möglichst ausgeschlossen werden kann (zum Beispiel in luftgepolsterte Umschläge).

5.7. Fristen / Vorhaltezeiten

Für die Datensicherung zur Wiederherstellung von IT-Systemen und für die Sicherung von Rohdaten müssen Vorhaltezeiten festgelegt werden.

Bei den geplanten Datensicherungssystemen wird die Vorhaltezeit maßgeblich dadurch bestimmt, wie lange Vollsicherungen im Datensicherungsbestand gespeichert werden können. Es ist eine Vorhaltezeit zu wählen, die für eine Wiederherstellung praktikabel und sinnvoll ist.
Bei einer Software Wiederherstellung aus dem Datensicherungsbestand (Vollsicherung und Konfiguration) sollte die Vollsicherung nicht älter als 45 Tage sein.

5.8. Vertraulichkeit und Integrität

Die Vertraulichkeit von Daten überträgt sich bei einer Datensicherung von der Datenquelle auf die Sicherungskopie. Bei der Zusammenführung von Sicherungskopien mit gleicher Vertraulichkeit auf einem Datenträger kann sich durch die Kumulation ein höherer Schutzbedarf der gespeicherten Daten ergeben.
Die Vertraulichkeit der IT-Systeme und Dateninhalte ist durch die Informationseigentümer festzulegen oder aus der Schutzbedarfsfeststellung abzuleiten.
Alle mit dem Datensicherungsverfahren erzeugten Sicherungen müssen auf den Quellensystemen und falls dort nicht möglich auf dem Datensicherungssystem nach Stand der Technik verschlüsselt gespeichert werden.
Beim Speichern müssen dedizierte Verzeichnisse erstellt werden, um eine Trennung der kumulierten Daten zu gewährleistet, damit kein höherer Vertraulichkeitsbedarf als auf den Quellensystemen erforderlich wird.
Bei der Speicherung der Datensicherungen muss sichergestellt sein, dass die Dateien einem Quellensystem eindeutig zugeordnet werden können. Jede Sicherungsdatei muss den Namen des Quellensystems, den Datumsstempel der Erstellung und eine eindeutige Dateiendung tragen. Sollte dies nicht möglich sein, muss dokumentiert werden in welcher Weise eine Zuordnung erfolgen kann (z.B. über Datensicherungs-Applikation).
Der Zugang und Zugriff auf das Datensicherungssystem zur Wahrnehmung der betrieblichen Aufgaben der Datensicherung muss an berechtigte Personen (mit Bezug zum Rollen- und Berechtigungskonzept) vergeben werden, die speziell für diese Rolle benannt werden.
Die Integrität der Datensicherungen gegen Fremdzugriff und Veränderung muss bei der Übertragung auf das Datensicherungssystem durch die Verwendung spezifischer Übertragungsprotokolle gewährleistet sein.

5.9. Dokumentation der Datensicherung

Die Dokumentation der automatischen Datensicherung erfolgt in Log-Dateien. Jede erfolgreiche und nicht erfolgreiche Datensicherung auf den Quellensystemen und auf dem Datensicherungssystem wird aufgezeichnet. Sollten sich Abweichung zu den Anforderungen ergeben, müssen diese durch die Stabstelle Datenschutz und Informationssicherheit bewertet und durch den Produktverantwortlichen dokumentiert werden.
Entsprechende Rückgabewerte und Event Logs müssen durch die eingesetzte Backup-Software, das Backup-Management und durch das gesicherte IT-System erzeugt werden. Bei der Dokumentation der Datensicherung in den Log-Dateien müssen Datum, Start- und Endzeit, Quellensystem- / Datensicherungs-Zielsystem, Name des Sicherungsfiles, Backupdauer und technische Informationen über die erfolgreiche / nicht erfolgreiche Datensicherung aufgeführt sein.

Alle Vorgänge bei der Datensicherung werden in Log-Dateien protokolliert, und sind Bestandteil der Log-Daten Sicherung. Die Überwachung der Log-Daten auf den Datensicherungssystemen sollte zentral erfolgen.
Die Datensicherungssysteme müssen in die Systemüberwachung der VAV eingebunden werden.

5.10. Automatische / manuelle Datensicherungen

Das automatische Backupsystem muss in seiner Kapazität so konzipiert werden, dass die Vorhaltung aller Datensicherungen möglich ist.
Es muss für jeden VAV Standort ein Sicherungssystem für Rohdaten und ein Sicherungssystem für Backupdaten implementiert werden, damit Quellensysteme des lokalen Standorts und die Quellensysteme des parallelen Standorts wechselseitig gesichert werden können. Hierbei ist darauf zu achten, dass Produktivdaten der Quellsysteme physisch getrennt von den Datensicherungssystemen gespeichert werden.
Jedes Datensicherungssystem muss selbst in die Datensicherung eingebunden werden. Bei dieser Datensicherung werden ausschließlich das Betriebssystem, die Konfiguration und die Backup-Anwendung berücksichtigt.
Sind manuelle Datensicherungen erforderlich, so sind diese über das Datensicherungssystem durchzuführen. Dabei müssen dieselben Verfahren angewendet werden wie in der automatischen Datensicherung. Die Auslagerung von Daten oder die Erstellung von „Recovery“ CD / DVD-Datenträger muss an den Datensicherungssystemen durchgeführt und protokolliert werden.
Datensicherung von mobilen IT-Systemen (Laptops) sollten durchgeführt werden. Es sollte ein Backup der Systeme für die Wiederherstellung nach einem Hardware- / Softwareausfall vorliegen.
Konfigurationsdaten müssen gesichert werden, wenn diese für den Betrieb der Hardware oder der Anwendungen erforderlich sind.

6. WIEDERHERSTELLUNG VON DATEN

6.1. Wiederherstellung von Daten ohne Datensicherung

Für IT-Systeme der VAV wird die Wiederherstellung ohne Datensicherung nicht betrachtet. Es wird davon ausgegangen, dass durch die Redundanz der IT-Systeme und der vorhandenen Datensicherung jederzeit die Möglichkeit besteht eine Datenbasis zu erzeugen und auf das wiederherzustellende IT-System aufzuspielen.
Damit bei IT-Systemen im Fall eines Teil- oder Totalverlustes der Datenbasis eine Wiederherstellung möglich ist, müssen am Standort Originaldatenträger der Hersteller, Datensicherungen und Software für die Wiederherstellung zur Verfügung stehen. Zur spezifischen Konfiguration muss die Systemdokumentation ebenfalls vorliegen.

6.2. Wiederherstellung von Daten aus der Datensicherung

Die Wiederherstellung von Daten auf Quellensystemen muss durch Rückspielen von Backup-Daten aus dem Datensicherungsbestand gewährleistet sein. Das Einspielen von Daten aus dem

Datensicherungsbestand muss mit vollständigen Datensicherungen (Vollbackups) und einzelnen Dateien auf die Quellensysteme möglich sein.
Es müssen betriebliche Verfahrensanweisungen und Arbeitsanweisungen für die Bereitstellung und das Einspielen der Daten beschrieben werden.
Für alle IT-Systeme, auf denen eine lokale Backup-Software zur Anwendung kommt, muss nach der Erstinstallation ein „Recovery“ Medium oder File erstellt werden. Nur mit diesen erstellten „Recovery“ Daten darf es möglich sein, das IT-System aus dem Datensicherungsbestand des Datensicherungssystems wiederherzustellen.
Für die vollständige Wiederherstellung von Quellensystemen sollten deren Originaldatenträger/-files und Datenträger / -files mit der eingesetzten Backup-Software für jedes IT-System zur Verfügung stehen. Nach einer Wiederherstellung der Grundkonfiguration von Originaldatenträgern/-files und Einbindung in die Infrastruktur ist die letzte Datensicherung aus den Datensicherungssystemen für die vollständige Wiederherstellung anzuwenden.

6.3. Minimaldatensicherungskonzept

Es werden alle notwendigen und erreichbaren Daten über eine automatische Datensicherung gesichert.
Werden neue und ergänzende IT-Systeme innerhalb der VAV eingeführt, müssen diese in die automatische Datensicherung aufgenommen werden.
Bei neuen IT-Systemen oder Applikationen, welche im Zuge eines Projekts eingeführt werden, muss ein Datensicherungskonzept erstellt und dieses im Betriebshandbuch dokumentiert werden. Vor Übergabe an die Linie muss die Datensicherungs- und Wiederherstellungsfähigkeit getestet werden.

6.4. Übung zur Datenwiederherstellung

Die Wiederherstellung von Daten mit Hilfe von Datensicherungsbeständen muss einmal jährlich und nach jeder Änderung des Datensicherungsverfahrens getestet werden. Hierbei muss zumindest einmal nachgewiesen werden, dass eine vollständige Datenwiederherstellung eines Gesamtdatenbestands eines Servers möglich ist. Zuständig für die Durchführung ist der jeweilige Produktverantwortliche in Absprache mit den interessierten Parteien.
Die Wiederherstellung von IT-Systemen mit neuer Hardware aus der Datensicherung ist nachzuweisen. Die einzelnen Prozeduren sind dokumentiert und müssen in die betrieblichen Prozesse mit den notwendigen Verfahrensanweisungen und Arbeitsanweisungen für eine Übung zur Wiederherstellung eingearbeitet werden.
Um das Verfahren der Datensicherung, die vorliegende Dokumentation und den Zeitaufwand zur Datenwiederherstellung an IT-Systemen testen zu können, müssen Systeme ausgewählt werden, die im Fehlerfall der Wiederherstellung die Verfügbarkeit der VAV Systemlandschaft nicht gefährden.
Werden Wiederherstellungsübungen an operativen IT-Systemen durchgeführt, muss gewährleistet sein, dass die Redundanz der gewählten IT-Systeme zur Verfügung steht und getestet wurde.
IT-Systeme wie Arbeitsstationen, die mehrfach zur Verfügung stehen, sollten zum Test des Datensicherungsverfahren und der vollständigen Wiederherstellung verwendet werden.
Stehen innerhalb der VAV Referenzsysteme (Entwicklungsebenen) zur Verfügung, müssen diese für die Datenwiederherstellung verwendet werden. Ist eine Wiederherstellung erfolgreich, kann eine entsprechende Übung in der operativen Umgebung durchgeführt werden.
Die organisatorischen und operativen Prozesse für eine Restaurierungsübung müssen zur Produktivsetzung erstellt sein.