

Familie: Access Control

Baselines:

Low

Moderate

High

Privacy

### Beschreibung

a. Entwicklung, Dokumentation und Weitergabe an [von der Organisation definierte Mitarbeiter oder Rollen]:

1. [Auswahl (eine oder mehrere): Organisationsebene; Auftrags-/Geschäftsprozessebene; Systemebene]

ZugriffskontrollRichtlinien, die:

(a) den Zweck, den Umfang, die Rollen, die Verantwortlichkeiten, die Verpflichtung des Managements, die Koordinierung zwischen den Organisationseinheiten und die Einhaltung der Vorschriften regelt; und

(b) mit den geltenden Gesetzen, Anordnungen, Direktiven, Verordnungen, Richtlinien, Standards und Leitlinien übereinstimmt; und

2. Verfahren zur Erleichterung der Umsetzung der ZugangskontrollRichtlinien und der damit verbundenen Zugangskontrollen;

b. Benennung eines [Beamten], der die Entwicklung, Dokumentation und Verbreitung der ZugangskontrollRichtlinien und -verfahren leitet; und

c. Überprüfung und Aktualisierung der aktuellen Zugangskontrolle:

1. Richtlinien [Häufigkeit] und folgende [Ereignisse]; und

2. Verfahren [Häufigkeit] und nach [Ereignissen].

### Ergänzende Hinweise

ZugangskontrollRichtlinien und -verfahren befassen sich mit den Kontrollen der AC-Familie, die in Systemen und Organisationen implementiert werden. Die Risikomanagementstrategie ist ein wichtiger Faktor bei der Festlegung solcher Strategien und Verfahren. Richtlinien und Verfahren tragen zur Gewährleistung von Sicherheit und Datenschutz bei. Daher ist es wichtig, dass Sicherheits- und Datenschutzprogramme bei der Entwicklung von Zugriffskontrollrichtlinien und -verfahren zusammenarbeiten. Richtlinien und Verfahren für Sicherheits- und Datenschutzprogramme auf Organisationsebene sind im Allgemeinen vorzuziehen und können den Bedarf an aufgaben- oder systemspezifischen Richtlinien und Verfahren überflüssig machen. Die Richtlinie kann Teil der allgemeinen Sicherheits- und DatenschutzRichtlinien sein oder aus mehreren Richtlinien bestehen, die die Komplexität von Organisationen widerspiegeln. Verfahren können für Sicherheits- und Datenschutzprogramme, für Aufgaben- oder Geschäftsprozesse und bei Bedarf auch für Systeme festgelegt werden. Verfahren beschreiben, wie die Richtlinien oder Kontrollen umgesetzt werden, und können sich an die Person oder Rolle richten, die Gegenstand des Verfahrens ist. Verfahren können in Plänen für Systemsicherheit und Datenschutz oder in einem oder mehreren separaten Dokumenten dokumentiert werden. Zu den Ereignissen, die eine Aktualisierung der Richtlinien und Verfahren für die Zugangskontrolle erforderlich machen können, gehören Beurteilungs- oder Prüfungsergebnisse, Sicherheitsvorfälle oder -verletzungen oder Änderungen von Gesetzen, Durchführungsverordnungen, Direktiven, Vorschriften, Richtlinien, Standards und Leitlinien. Die bloße Wiederholung von Kontrollen stellt keine organisatorische Richtlinie oder Prozedur dar.

### Verwandte Kontrollen

IA-01, PM-09, PM-24, PS-08, SI-12

Familie: Identification and Authentication

Baselines:

Low

Moderate

High

Privacy

## Beschreibung

- a. Entwicklung, Dokumentation und Weitergabe an [von der Organisation definierte Mitarbeiter oder Rollen]:
  1. [Auswahl (eine oder mehrere): Organisationsebene; Auftrags-/Geschäftsprozessebene; Systemebene] Identifizierungs- und Authentifizierungsrichtlinien, die:
    - (a) den Zweck, den Umfang, die Rollen, die Verantwortlichkeiten, die Verpflichtung des Managements, die Koordination zwischen den Organisationseinheiten und die Einhaltung der Vorschriften regelt; und
    - (b) mit den geltenden Gesetzen, Anordnungen, Direktiven, Verordnungen, Richtlinien, Standards und Leitlinien übereinstimmt; und
  2. Verfahren zur Erleichterung der Umsetzung der Identifizierungs- und Authentifizierungsrichtlinien und der damit verbundenen Identifizierungs- und Authentifizierungskontrollen;
- b. Benennung eines [Beamten], der die Entwicklung, Dokumentation und Verbreitung der Identifizierungs- und Authentifizierungsrichtlinien und -verfahren leitet; und
- c. Überprüfung und Aktualisierung der aktuellen Identifizierungs- und Authentifizierungsrichtlinien:
  1. Richtlinien [Häufigkeit] und folgende [Ereignisse]; und
  2. Verfahren [Häufigkeit] und nach [Ereignissen].

## Ergänzende Hinweise

Identifizierungs- und Authentifizierungsrichtlinien und -verfahren betreffen die Kontrollen in der IA-Familie, die in Systemen und Organisationen implementiert werden. Die Risikomanagementstrategie ist ein wichtiger Faktor bei der Festlegung solcher Strategien und Verfahren. Richtlinien und Verfahren tragen zur Gewährleistung von Sicherheit und Datenschutz bei. Daher ist es wichtig, dass Sicherheits- und Datenschutzprogramme bei der Entwicklung von Identifizierungs- und Authentifizierungsrichtlinien und -verfahren zusammenarbeiten. Richtlinien und Verfahren für Sicherheits- und Datenschutzprogramme auf Organisationsebene sind im Allgemeinen vorzuziehen und können den Bedarf an missions- oder systemspezifischen Richtlinien und Verfahren überflüssig machen. Die Richtlinie kann Teil der allgemeinen Sicherheits- und Datenschutzrichtlinie sein oder aus mehreren Richtlinien bestehen, die die Komplexität von Organisationen widerspiegeln. Verfahren können für Sicherheits- und Datenschutzprogramme, für Aufgaben- oder Geschäftsprozesse und bei Bedarf auch für Systeme festgelegt werden. Verfahren beschreiben, wie die Richtlinien oder Kontrollen umgesetzt werden, und können sich an die Person oder Rolle richten, die Gegenstand des Verfahrens ist. Verfahren können in Plänen für Systemsicherheit und Datenschutz oder in einem oder mehreren separaten Dokumenten dokumentiert werden. Zu den Ereignissen, die eine Aktualisierung der Identifizierungs- und Authentifizierungsrichtlinien und -verfahren erforderlich machen können, gehören Beurteilungs- oder Prüfungsergebnisse, Sicherheitsvorfälle oder -verletzungen oder Änderungen der geltenden Gesetze, Durchführungsverordnungen, Direktiven, Vorschriften, Richtlinien, Standards und Leitlinien. Die bloße Wiederholung von Kontrollen stellt keine organisatorische Richtlinie oder Prozedur dar.

## Verwandte Kontrollen

AC-01, PM-09, PS-08, SI-12

Familie: Program Management

Baselines:

High

## Beschreibung

- a. Entwickelt eine umfassende Strategie zur Verwaltung:
  - 1. Sicherheitsrisiken für den Betrieb und die Vermögenswerte der Organisation, für Einzelpersonen, andere Organisationen und die Nation, die mit dem Betrieb und der Nutzung der Systeme der Organisation verbunden sind; und
  - 2. Datenschutzrisiken für Einzelpersonen, die sich aus der autorisierten Verarbeitung von personenbezogenen Daten ergeben;
- b. Umsetzung der Risikomanagementstrategie in der gesamten Organisation; und
- c. Überprüfung und Aktualisierung der Risikomanagementstrategie [häufig] oder bei Bedarf, um organisatorischen Veränderungen Rechnung zu tragen.

## Ergänzende Hinweise

Eine organisationsweite Risikomanagement-Strategie umfasst die Risikotoleranz der Organisation in Bezug auf Sicherheit und Datenschutz, Strategien zur Risikominderung in Bezug auf Sicherheit und Datenschutz, akzeptable Risikobewertungsmethoden, ein Verfahren zur Bewertung von Sicherheits- und Datenschutzrisiken in der gesamten Organisation im Hinblick auf die Risikotoleranz der Organisation sowie Ansätze zur Risikoüberwachung im Laufe der Zeit. Der ranghöchste Verantwortliche für das Risikomanagement (Behördenleiter oder benannter Beamter) stimmt die Prozesse des Informationssicherheitsmanagements mit den strategischen, operativen und budgetären Planungsprozessen ab. Die Risikoexekutivfunktion, die vom leitenden Verantwortlichen für das Risikomanagement geleitet wird, kann die konsequente Anwendung der Risikomanagementstrategie in der gesamten Organisation erleichtern. Die Risikomanagementstrategie kann durch sicherheits- und datenschutzbezogene Beiträge aus anderen Quellen, sowohl intern als auch extern, informiert werden, um sicherzustellen, dass die Strategie breit angelegt und umfassend ist. Die in [PM-30](#pm-30) beschriebene Risikomanagementstrategie für die Lieferkette kann ebenfalls nützliche Beiträge für die organisationsweite Risikomanagementstrategie liefern.

## Verwandte Kontrollen

AC-01, AU-01, AT-01, CA-01, CA-02, CA-05, CA-06, CA-07, CM-01, CP-01, IA-01, IR-01, MA-01, MP-01, PE-01, PL-01, PL-02, PM-02, PM-08, PM-18, PM-28, PM-30, PS-01, PT-01, PT-02, PT-03, RA-01, RA-03, RA-09, SA-01, SA-04, SC-01, SC-38, SI-01, SI-12, SR-01, SR-02

Familie: Program Management

Baselines:

High

## Beschreibung

Einrichtung eines Gremiums für Datenintegrität mit folgenden Aufgaben:

- a. Prüfung von Vorschlägen zur Durchführung eines Abgleichprogramms oder zur Teilnahme an einem solchen; und
- b. Jährliche Überprüfung aller Abgleichprogramme, an denen die Behörde teilgenommen hat.

## Ergänzende Hinweise

Ein Data Integrity Board ist ein Gremium aus hochrangigen Beamten, das vom Leiter einer Bundesbehörde ernannt wird und unter anderem dafür verantwortlich ist, die Vorschläge der Behörde zur Durchführung oder Teilnahme an einem Abgleichsprogramm zu prüfen und eine jährliche Überprüfung aller Abgleichsprogramme durchzuführen, an denen die Behörde teilgenommen hat. Im Allgemeinen ist ein Abgleichsprogramm ein computergestützter Vergleich von Datensätzen aus zwei oder mehr automatisierten [PRIVACT](#18e71fec-c6fd-475a-925a-5d8495cf8455) Datensystemen oder einem automatisierten System von Datensätzen und automatisierten Datensätzen, die von einer nicht-bundesstaatlichen Behörde (oder deren Vertreter) geführt werden. Ein Abgleichsprogramm bezieht sich entweder auf bundesstaatliche Leistungsprogramme oder auf bundesstaatliche Personal- oder Gehaltsabrechnungsdaten. Dem Data Integrity Board gehören mindestens der Generalinspektor der Behörde (falls vorhanden) und der leitende Beamte der Behörde für Datenschutz an.

## Verwandte Kontrollen

AC-04, PM-19, PM-23, PT-02, PT-08

Familie: Personnel Security

Baselines:

Low

Moderate

High

## Beschreibung

- a. Anwendung eines formellen Sanktionsverfahrens für Personen, die sich nicht an die festgelegten Richtlinien und Verfahren zur Informationssicherheit und zum Datenschutz halten; und
- b. Benachrichtigung [des Personals oder der Rollen] innerhalb [des Zeitraums], wenn ein formelles Sanktionsverfahren gegen einen Mitarbeiter eingeleitet wird, unter Angabe der sanktionierten Person und des Grundes für die Sanktion.

## Ergänzende Hinweise

Organisatorische Sanktionen spiegeln geltende Gesetze, Durchführungsverordnungen, Direktiven, Vorschriften, Richtlinien, Standards und Leitlinien wider. Sanktionsverfahren werden in Zugangsvereinbarungen beschrieben und können Teil der allgemeinen PersonalRichtlinien von Organisationen sein und/oder in Sicherheits- und Datenschutzrichtlinien festgelegt werden. Organisationen konsultieren das Office of the General Counsel zu Fragen der Mitarbeitersanktionen.

## Verwandte Kontrollen

PL-04, PM-12, PS-06, PT-01

Familie: System and Information Integrity

Baselines:

Low

Moderate

High

Privacy

## Beschreibung

Verwaltung und Aufbewahrung von Informationen innerhalb des Systems und von Informationen, die aus dem System ausgegeben werden, in Übereinstimmung mit den geltenden Gesetzen, Durchführungsverordnungen, Direktiven, Vorschriften, Richtlinien, Standards, Richtlinien und betrieblichen Anforderungen.

## Ergänzende Hinweise

Die Anforderungen an die Informationsverwaltung und -aufbewahrung decken den gesamten Lebenszyklus von Informationen ab und reichen in einigen Fällen über die Entsorgung des Systems hinaus. Zu den aufzubewahrenden Informationen können auch Richtlinien, Verfahren, Pläne, Berichte, Daten, die bei der Durchführung von Kontrollen anfallen, und andere Arten von Verwaltungsinformationen gehören. Die National Archives and Records Administration (NARA) stellt Bundesrichtlinien und Leitlinien zur Aufbewahrung von Unterlagen und Zeitplänen zur Verfügung. Wenn eine Organisation über ein Büro für die Verwaltung von Unterlagen verfügt, sollten Sie sich mit den Mitarbeitern der Archivverwaltung abstimmen. Zu den Aufzeichnungen, die aus den Ergebnissen implementierter Kontrollen hervorgehen und möglicherweise verwaltet und aufbewahrt werden müssen, gehören unter anderem: Alle XX-1, [AC-6(9)](#ac-6.9), [AT-4](#at-4), [AU-12](#au-12), [CA-2](#ca-2), [CA-3](#ca-3), [CA-5](#ca-5), [CA-6](#ca-6), [CA-7](#ca-7), [CA-8](#ca-8), [CA-9](#ca-9), [CM-2](#cm-2), [CM-3](#cm-3), [CM-4](#cm-4), [CM-6](#cm-6), [CM-8](#cm-8), [CM-9](#cm-9), [CM-12](#cm-12), [CM-13](#cm-13), [CP-2](#cp-2), [IR-6](#ir-6), [IR-8](#ir-8), [MA-2](#ma-2), [MA-4](#ma-4), [PE-2](#pe-2), [PE-8](#pe-8), [PE-16](#pe-16), [PE-17](#pe-17), [PL-2](#pl-2), [PL-4](#pl-4), [PL-7](#pl-7), [PL-8](#pl-8), [PM-5](#pm-5), [PM-8](#pm-8), [PM-9](#pm-9), [PM-18](#pm-18), [PM-21](#pm-21), [PM-27](#pm-27), [PM-28](#pm-28), [PM-30](#pm-30), [PM-31](#pm-31), [PS-2](#ps-2), [PS-6](#ps-6), [PS-7](#ps-7), [PT-2](#pt-2), [PT-3](#pt-3), [PT-7](#pt-7), [RA-2](#ra-2), [RA-3](#ra-3), [RA-5](#ra-5), [RA-8](#ra-8), [SA-4](#sa-4), [SA-5](#sa-5), [SA-8](#sa-8), [SA-10](#sa-10), [SI-4](#si-4), [SR-2](#sr-2), [SR-4](#sr-4), [SR-8](#sr-8).

## Verwandte Kontrollen

AC-16, AU-05, AU-11, CA-02, CA-03, CA-05, CA-06, CA-07, CA-09, CM-05, CM-09, CP-02, IR-08, MP-02, MP-03, MP-04, MP-06, PL-02, PL-04, PM-04, PM-08, PM-09, PS-02, PS-06, PT-02, PT-03, RA-02, RA-03, SA-05, SA-08, SR-02