DGI® Deutsche Gesellschaft für Informationssicherheit AG

Glossar

für die Nutzung der Dokumente für die Umsetzung von Managementsystemen

Begriffsübersicht

Abnahmetest

Ein Abnahmetest beschreibt ein Testmodell zum Überprüfen, ob und inwieweit aus Sicht des Kunden alle Rahmenbedingungen gegeben sind, um einen IT-Service nach einer Entwicklung oder Änderung in Betrieb nehmen zu dürfen. Bei einem Abnahmetest erfolgt vor dem Starten eines IT-Service stets eine verbindliche Bestätigung (Abnahme) des Kunden, dass die Datenverarbeitung bzw. das IT-System die Anforderungen erfüllt.

Anwendung

Eine Anwendung oder auch Software, stellt die benötigten Funktionen für die IT-Services bereit. Jede Anwendung kann Teil eines oder mehrerer IT-Services sein. Eine Anwendung wird auf einem oder mehreren Servern oder Clients ausgeführt.

Archivierung

Der Begriff Archivierung beschreibt die dauerhafte und unveränderbare Speicherung von Daten und Datenträgern auf eine strukturierte Art, sodass ein schnelles und einfaches Wiederauffinden ermöglicht ist.

Asset

Ein Asset bezeichnet jedwede Ressource oder Fähigkeit. Die Assets eines Service Providers umfassen alle Elemente, die zur Erbringung eines Service beitragen können. Es werden folgende Asset-Typen unterschieden: Management, Organisation, Prozess, Wissen, Mitarbeiter, Informationen, Anwendungen, Infrastruktur und finanzielles Kapital.

Authentisierung

Authentisierung bezeichnet den Nachweis oder die Überprüfung der Authentizität. Die Authentisierung einer Identität kann u. a. durch Passwort-Eingabe, Chipkarte oder Biometrie erfolgen, die Authentisierung von Daten z. B. durch kryptographische Signaturen.

Audit

Ein Audit ist eine systematische und unabhängige Untersuchung, um festzustellen ob die vereinbarten Anforderungen, aus relevanten Normen und Standards, an Prozesse, Anweisungen und Regelungen sowie die Dokumentation erfüllt werden. Im Rahmen der Durchführung eines Audits werden Feststellungen bezüglich der Konformität, der Nichtkonformität und der Verbesserungspotentiale getroffen.

Aufrechterhaltung der Betriebsfähigkeit der IT

Die Aufrechterhaltung der Betriebsfähigkeit der IT bezeichnet die Fähigkeit der Organisation die geplanten oder vereinbarten Leistungen für den Betrieb des IT-gestützten Geschäftsbetriebs wie gefordert, insbesondere während einer Beeinträchtigung des Betriebs, fortlaufend zu erbringen, Maßnahmen für die Reaktion auf ungeplante und unerwünschte Beeinträchtigungen sowie die Bewältigung eines IT-Notfalls frühestmöglich und bestmöglich durchzuführen.

Authentizität

Mit dem Begriff Authentizität wird die Eigenschaft bezeichnet, die gewährleistet, dass ein Kommunikationspartner tatsächlich derjenige ist, der er vorgibt zu sein. Bei authentischen Informationen ist sichergestellt, dass sie von der angegebenen Quelle erstellt wurden. Der Begriff wird nicht nur verwendet, wenn die Identität von Personen geprüft wird, sondern auch bei IT-Komponenten oder Anwendungen.

Autorisierung

Bei einer Autorisierung wird geprüft, ob eine Person, IT-Komponente oder Anwendung zur Durchführung einer bestimmten Handlung berechtigt ist.

Backup

siehe Datensicherung

Basis-Absicherung

Der Begriff Basis-Absicherung bezeichnet eine Vorgehensweise des IT-Grundschutz zur grundlegenden Erst-Absicherung über alle Geschäftsprozesse bzw. Fachverfahren einer Organisation.

Basis-Anforderung

siehe Sicherheitsanforderung

Baustein

Das IT-Grundschutz-Kompendium enthält für unterschiedliche Vorgehensweisen, Komponenten und IT-Systeme Erläuterungen zur Gefährdungslage, Sicherheitsanforderungen und weiterführende Informationen, die jeweils in einem Baustein zusammengefasst sind. Die grundlegende Struktur des IT-Grundschutz-Kompendiums sieht eine Unterteilung in prozess- und systemorientierte Bausteine vor, zudem sind sie nach Themen in ein Schichtenmodell einsortiert.

BCP

siehe Business Continuity Plan / Business Continuity Planning

BCM

siehe Business Continuity Management

BCMS

siehe Business Continuity Management System

Bedrohung

Eine Bedrohung ist ein Umstand oder Ereignis, durch den oder das ein Schaden entstehen kann. Der Schaden bezieht sich dabei auf einen konkreten Wert wie Vermögen, Wissen, Gegenstände oder Gesundheit und kann die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen beeinträchtigen. Beispiele für Bedrohungen sind höhere Gewalt, menschliche Fehlhandlungen, technisches Versagen oder vorsätzliche Handlungen. Aus Bedrohungslagen in Verbindung mit Schwachstellen können sich konkrete Gefährdungen ergeben.

Beeinträchtigung

Als Beeinträchtigung, Im Kontext der Betriebsfähigkeit der IT, wird ein Ereignis mit möglichen ungeplanten oder unerwünschten Auswirkungen für die Organisation beim Betrieb der IT-gestützten Geschäftsprozesse verstanden.

Benutzerkennung

Die Benutzerkennung bezeichnet einen Teil der Authentifizierung, mit dem sich der Benutzer einem System gegenüber identifiziert.

Benutzerrecht

Das Benutzerrecht bezeichnet die Zugangs- und Zugriffsrechte auf IT-Systeme, Anwendungen und Netzwerke.

Benutzerrolle

Eine Benutzerrolle, auch Rolle, bezeichnet die einheitliche Zuordnung von Berechtigungen für Nutzer auf Basis gleicher bzw. ähnlicher Aufgabenstellungen, um dieselben einzelnen Rechte direkt zuweisen zu können.

BIA

siehe Business Impact Analyse

Bring Your Own Device

Bring Your Own Device (BYOD) regelt, auf welche Weise Beschäftigte ihre eigenen elektronischen Geräte (Smartphones, Notebooks, Tablets) nutzen dürfen. BYOD soll den Nutzern eine größere Wahlfreiheit bei der Auswahl von technischen Geräten bringen und der Organisation eine bessere Orientierung an persönlichen Bedürfnissen ermöglichen.

Build

Ein Build beschreibt die Aktivität in Bezug auf die Gruppierung einer Reihe von Configuration Items als Teil eines IT-Service. Der Begriff bezeichnet auch ein Release, das zur Verteilung freigegeben ist, etwa ein Server-Build oder ein Laptop-Build.

Business Continuity Management

Business Continuity Management (BCM) bezeichnet alle organisatorischen, technischen und personellen Maßnahmen, die zur Fortführung des Kerngeschäfts einer Organisation nach Eintritt eines Notfalls dienen. Weiterhin unterstützt BCM die sukzessive Fortführung der Geschäftsprozesse bei länger anhaltenden Ausfällen oder Störungen.

Business Continuity Management System

Das Business Continuity Management System (BCMS) dient der Einführung der systematischen Steuerung und der Umsetzung von Maßnahmen für die Sicherstellung der Aufrechterhaltung der Betriebsfähigkeit (Resilienz). Die Steuerung des BCMS umfasst die Umsetzung der Phasen Planung, Unterstützung, Betrieb, Bewertung der Leistung und fortlaufende Verbesserung, den Aufbau der Dokumentation und deren Erstellung, Aktualisierung, Pflege und Lenkung sowie die Entwicklung und Umsetzung der Verfahren, Prozesse, Anweisungen und Regelungen.

Business Continuity Plan

Ein Business Continuity Plan (BCP) definiert die Schritte, die für eine Wiederherstellung der Betriebsfähigkeit, insbesondere der IT-gestützten Geschäftsprozesse, nach einer Störung erforderlich sind. Ein BCP identifiziert darüber hinaus die Bedingungen für das Auslösen des BCP, die beteiligten Personen sowie deren Verantwortlichkeiten. Grundsätzlich beinhaltet ein BCP die Sofortmaßnahmen sowie die Maßnahmen für die Wiederherstellung der Betriebsfähigkeit.

Business Continuity Planning

Business Continuity Planning (BCP) bezeichnet das Planen, die Umsetzung sowie die Aufrechterhaltung und Verbesserung des Zusammenwirkens von der Aufnahme von Reaktionsplänen für Sofortmaßnahmen sowie von Reaktionsplänen der Wiederherstellung und des Wiederanlaufs aus Notbetriebsszenarien heraus, um den ordnungsgemäßen, sicheren und konformen Geschäftsbetrieb fortsetzen zu können.

Business Impact Analyse

Eine Business Impact Analyse (BIA) ist eine Analyse zur Ermittlung von potenziellen direkten und indirekten Folgeschäden für eine Organisation, die durch das Auftreten eines Ausfalls eines oder mehrerer Geschäftsprozesse verursacht werden. Die BIA identifiziert insbesondere kritische Ressourcen, Wiederanlauf- und Wiederherstellungsparameter sowie die Auswirkungen von ungeplanten Geschäftsunterbrechungen.

BYOD

siehe Bring Your Own Device

Change

Ein Change bezeichnet das Hinzufügen, Modifizieren oder Entfernen eines autorisierten, geplanten oder unterstützten Service oder einer Servicekomponente und der zugehörigen Dokumentation, das Auswirkungen auf die IT-Services haben könnte.

Change-Vorschlag

Ein Change-Vorschlag ist ein Dokument, das einen vorgeschlagenen größeren Change beinhaltet, etwa die Neueinführung eines Service oder umfangreiche Änderungen an bestehenden Services. Ein Change-Vorschlag dient der besseren Kommunikation von Changes zur Beurteilung von Risiko, Auswirkungen und Machbarkeit.

CI

siehe Configuration Item

Client

Als Client wird Soft- oder Hardware bezeichnet, die bestimmte Dienste von einem Server in Anspruch nehmen kann. Häufig steht der Begriff Client für einen Arbeitsplatzrechner, der auf Daten und Programme von Servern zugreift.

Cloud

Cloud Computing ist ein Modell, das es erlaubt bei Bedarf, jederzeit über ein Netz auf einen geteilten Pool von konfigurierbaren Rechnerressourcen (z. B. Netze, Server, Speichersysteme, Anwendungen und Dienste) zuzugreifen, die schnell und definiertem Managementaufwand oder Serviceprovider-Interaktion zur Verfügung gestellt werden können.

CMDB

siehe Configuration Management Database

CMS

siehe Configuration Management System

Configuration Item

Der Begriff Configuration Item (Konfigurationselement, CI) beschreibt alle Komponenten und andere Service Assets, die gemanagt werden müssen, um einen IT-Service bereitstellen zu können. Informationen zu den einzelnen CIs werden in einem Configuration Record innerhalb des Configuration Management Systems (CMS) erfasst und über den gesamten Lebenszyklus hinweg vom Service Asset and Configuration Management (SACM) gemanagt. Cis unterstehen der Steuerung und Kontrolle des Change Management. CIs umfassen vor allem IT-Services, Hardware, Software, Gebäude, Personen und formale Dokumentationen, beispielsweise zum Prozess und zu Service Level Agreements (SLA).

Configuration Management Database

Eine Configuration Management Database (CMDB) beschreibt eine Datenbank, die verwendet wird, um Configuration Records während ihres gesamten Lebenszyklus zu speichern. Eine CMDB speichert Attribute von Configuration Items (CI) sowie Beziehungen zu anderen CIs.

Configuration Management System

Ein Configuration Management System (CMS) beschreibt eine Kombination von Tools und Daten, die zum Sammeln, Speichern, Managen, Aktualisieren, Analysieren und zur Präsentation von Daten zu allen Configuration Items / Service Assets und deren Beziehungen eingesetzt wird. Ein CMS kann ein oder mehrere physikalische Configuration Management Databases (CMDB) verwalten.

Critical Success Factor

Als Critical Success Factor werden die für den IT-Betrieb kritischen Faktoren bezeichnet, die eine Identifikation der ungeplanten und unerwünschten Ergebnisse der Leistungs- und Qualitätserbringung zu ermöglichen sowie im Umkehrschluss die Messwerte für die Bestimmung und Festlegung der Key Performance Indicator (Schlüsselkennzahlen) für die Steuerung des ordnungsgemäßen, sicheren und konformen Geschäftsbetriebs sicherzustellen.

CSF

siehe Critical Success Factor

Cyber

Cyber bezeichnet den virtuellen Raum, auch Cyber-Raum, aller auf Datenebene vernetzten bzw. vernetzbaren informationstechnischen Systeme. Dem Cyber-Raum liegt als öffentlich zugängliches Verbindungsnetz das Internet zugrunde, welches durch beliebige andere Datennetze erweitert werden kann.

Cyber-Sicherheit

Cyber-Sicherheit befasst sich mit allen Aspekten der Informationssicherheit im Cyber-Raum.

Datenschutz

Datenschutz bezeichnet die Einhaltung der Anforderungen zur Sicherstellung der informationellen Selbstbestimmung (Persönlichkeitsrecht) einer natürlichen Person. Dies umfasst insbesondere die Sicherstellung des datenschutzkonformen Umgangs mit analogen und digitalen personenbezogenen Daten.

Datenschutzmanagement

Datenschutzmanagement bezeichnet das Prozesswesen, um die Umsetzung der gesetzlichen Anforderungen des Datenschutzes bei der Planung, Einrichtung, dem Betrieb und der Außerbetriebnahme von Verfahren bei der Verarbeitung personenbezogener Daten sicherzustellen.

Datensicherheit

siehe IT-Sicherheit

Datensicherung

Datensicherung bezeichnet den Schutz vor Datenverlust durch die Erstellung von Sicherungskopien von vorhandenen Datenbeständen. Datensicherung umfasst alle technischen und organisatorischen Maßnahmen zur Sicherstellung der Verfügbarkeit, Integrität und Konsistenz der Systeme einschließlich der auf diesen Systemen gespeicherten und für Verarbeitungszwecke genutzten Daten, Programme und Prozeduren.

Definitive Media Library

Eine Definitive Media Library (DML) beschreibt einen physischen oder logischen Aufbewahrungsort, an dem alle maßgeblichen autorisierten Originalversionen aller Software-Master-Kopien aufbewahrt werden.

Deployment

Ein Deployment bezeichnet die Aktivität, die für den Übergang u. a. neuer oder geänderter Hardware, Software, Dokumentation oder Prozesse in die Live-Umgebung verantwortlich ist. Das Deployment ist Teil des Release and Deployment Management Prozesses.

Desaster Recovery

Desaster Recovery als Teil des Business Continuity Management bezeichnet insbesondere die Gewährleistung der Wiederherstellung der Datenbanken und Daten sowie der Infrastruktur, der IT-Infrastruktur und der Hardware, unter Berücksichtigung der vereinbarten Wiederanlauf- und Wiederherstellungsparameter.

Disaster Recovery

siehe Desaster Recovery

DML

siehe Definitive Media Library

Dokumentierte Information

Der Begriff dokumentierte Information beschreibt eine Information, die von einer Organisation gelenkt und aufrechterhalten werden muss und das Medium, auf dem sie enthalten ist. Eine dokumentierte Information kann in jeglichem Format oder Medium vorliegen, sowie aus jeglicher Quelle stammen.

Dritte

Ein Dritter ist jede Person oder Stelle außerhalb der verantwortlichen juristischen Person.

Emergency Change

Ein Emergency Change (auch Notfall-Change) ist ein Change, der so bald wie möglich eingeführt werden muss, beispielsweise um einen Major Incident zu lösen, oder ein Sicherheits-Patch zu installieren. Der Change Management Prozess bietet in der Regel ein bestimmtes Verfahren für die Behandlung von Notfall-Changes.

Entsorgung

Der Begriff Entsorgung beschreibt das Vernichten oder Zerstören von Informationen auf analogen Dokumenten und digitalen Datenträgern.

Event

Der Begriff Event beschreibt eine Statusänderung, die für das Management eines Configuration Item oder IT-Service von Bedeutung ist. Der Begriff Event bezeichnet darüber hinaus einen Alarm oder eine Benachrichtigung durch einen IT-Service, ein Configuration Item oder ein Monitoring Tool. Bei Events müssen in der Regel die Mitarbeiter des IT-Betriebs aktiv werden. Häufig führen Events zur Erfassung von Incidents.

Event Record

Ein Event Record ist ein Datensatz zur Beschreibung einer Statusänderung, die für die Verwaltung eines Configuration Items oder Services von Bedeutung ist.

Fernzugang

Mit Fernzugang wird die Berechtigungsaktivität für die Nutzung von Netzwerken, IT-Systemen und System-Komponenten bezeichnet, sofern der Zugang von einem externen Standort aus erfolgt.

Fernzugriff

Mit Fernzugriff wird die Berechtigungsaktivität für die Nutzung von Informationen und Daten bezeichnet, sofern der Zugang von einem externen Standort aus erfolgt.

Firewall

Der Begriff Firewall beschreibt ein System aus soft- und hardwaretechnischen Komponenten, um IP-Netze sicher zu koppeln. Eine Firewall kontrolliert den Datenfluss zwischen einem internen und einem externen Netzwerk. Alle Daten, die das Netz verlassen, können ebenso überprüft werden, wie die, die hineinwollen.

Folgeschädenabschätzung

siehe Business Impact Analyse

Funktionalitätsprüfungen

Bei einer Funktionalitätsprüfung wird geprüft, ob und inwieweit alle geforderten Schnittstellen und Funktionen eingesetzt werden können und inwieweit diese die geplanten Ergebnisse ermöglichen.

Gefahr

Als Gefahr wird die übergeordnete Situation bezeichnet, die eine negative Auswirkung zur Folge haben kann. Sofern diese negative Auswirkung spezifisch bestimmt werden kann (räumlich und zeitlich nach Art, Größe und Richtung) wird sie als Gefährdung verstanden.

Gefährdung

Als Gefährdung wird eine Situation bezeichnet, die eine spezifisch bestimmbare negative Auswirkung zur Folge haben kann (räumlich und zeitlich nach Art, Größe und Richtung).

Geschäftsfortführungsplan

siehe Business Continuity Plan

Geschäftsprozess

Ein Geschäftsprozess ist eine Menge logisch verknüpfter Einzeltätigkeiten, die ausgeführt werden, um ein bestimmtes geschäftliches oder betriebliches Ziel zu erreichen.

Grundwerte

Als Grundwerte, auch Schutzziele, der Informationssicherheit werden insbesondere folgende bezeichnet

- Vertraulichkeit: Nur berechtigte Personen sind in der Lage schutzwürdige Daten zu nutzen
- Integrität: Daten können nicht verändert, gelöscht oder hinzugefügt werden
- Verfügbarkeit: Daten stehen zu definierten Zeitpunkten im definierten Umfang zur Verfügung
- Weitere Grundwerte sind beispielsweise die Authentizität, die Verbindlichkeit oder die Nichtabstreitbarkeit.

ICS

siehe Industrial Control System

ICT Readiness for Business Continuity

ICT Readiness for Business Continuity als Teil des Business Continuity Management bezeichnet insbesondere die Gewährleistung der Wiederherstellung der ICT-Services, Hardware, Software, ICT-Infrastrukturkomponenten und technischen Schnittstellen der ICT-Systeme sowie der Telekommunikation, unter Berücksichtigung der vereinbarten Wiederanlauf- und Wiederherstellungsparameter.

Incident

Ein Incident bezeichnet eine nicht geplante Unterbrechung eines IT-Service oder eine Qualitätsminderung eines IT-Service. Auch ein Ausfall eines Configuration Item ohne bisherige Auswirkungen auf einen Service ist ein Incident, wie ein Ausfall einer oder mehrerer Festplatten in einer gespiegelten Partition.

Industrial Control System

Ein industrielles Steuerungssystem (Industrial Control System, ICS) ist eine Hard- und Softwarelösung zur Automatisierung. Elementare Bestandteile eines ICS sind Sensoren, Aktoren und deren Vernetzung, um die Steuerung von industriellen Prozessen zu ermöglichen und zu managen.

Informationssicherheit

Informationssicherheit hat den Schutz sämtlicher Informationen als Ziel. Dabei können Informationen in jeglicher Art, analog oder digital, vorliegen. Selbst nicht dokumentierte Informationen sind Gegenstand der Betrachtung von Maßnahmen zur Informationssicherheit. Informationssicherheit und IT-Sicherheit sind nicht synonym zu verwenden.

Informationssicherheitsbeauftragter

Die Bezeichnung Informationssicherheitsbeauftragter (ISB) betitelt eine Person mit Fachkompetenz für das Management von Informationssicherheit, die für Aspekte rund um die Informationssicherheit zuständig ist und sich verantwortlich für das Informationssicherheitsmanagement zeichnet. Abhängig von der Organisationsform kann eine Unterscheidung zwischen dem ISB und dem IT-Sicherheitsbeauftragten getroffen werden.

Informationssicherheitsereignis

Ein Informationssicherheitsereignis beschreibt eine Schwachstelle, die mit dem in Zusammenhang stehenden Ereignis zukünftig einen Informationssicherheitsvorfall zur Folge haben kann.

Informationssicherheitsleitlinie

Die Informationssicherheitsleitlinie beschreibt, für welche Zwecke, mit welchen Mitteln und mit welchen Strukturen Informationssicherheit innerhalb der Organisation hergestellt werden soll. Sie beinhaltet die von der Organisation angestrebten Informationssicherheitsziele sowie die avisierte Sicherheitsstrategie.

Informationssicherheitsmanagementsystem

Ein Informationssicherheitsmanagementsystem (ISMS) bestimmt den Aufbau einer Organisation, um die Steuerung, die Kontrolle sowie die kontinuierliche Verbesserung und Aufrechterhaltung der erforderlichen Dokumentationen und Prozesse sicherzustellen.

Informationssicherheitsvorfall

Ein Informationssicherheitsvorfall beschreibt eine einzelne oder eine Reihe von unerwünschten oder unerwarteten Informationssicherheitsereignissen, welche die Verfügbarkeit, Vertraulichkeit oder Integrität der Informations- und Telekommunikationstechnik (ITK) einschränken und bei denen eine erhebliche Wahrscheinlichkeit besteht, dass Geschäftsprozesse, Teilprozesse und/oder unterstützende Prozesse bzw. deren Ressourcen beeinträchtigt werden und Schäden für die Organisation entstehen oder entstehen können.

Informationsverbund

Unter einem Informationsverbund ist die Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Objekten zu verstehen, die der Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dienen. Ein Informationsverbund kann die gesamte Organisation oder einzelne abgrenzbare Bereiche umfassen.

Integrität

Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Die Sicherstellung der Integrität ermöglicht es, dass Daten vollständig und unverändert sind.

IRBC

siehe ICT Readiness for Business Continuity

ISB

siehe Informationssicherheitsbeauftragter

ISMS

siehe Informationssicherheitsmanagementsystem

ITSiBe

siehe IT-Sicherheitsbeauftragter

ITSM

siehe IT-Servicemanagement

IT-Compliance

Die IT-Compliance stellt die Einhaltung der standort- und branchenspezifischen Rechtsvorschriften, Normen und Standards sowie des Vertragswesens sicher und betrachtet deren Wechselbeziehungen mit dem IT-/TK-Betrieb.

IT-Governance

Die IT-Governance stellt die Einhaltung der Organisationsstrategie und -ziele sicher und lenkt die Aufbau- und Ablauforganisation des IT-/TK-Betriebs.

IT-Grundschutz-Check

Der Begriff IT-Grundschutz-Check bezeichnet im IT-Grundschutz die Überprüfung dessen, ob die nach IT-Grundschutz empfohlenen Anforderungen in einer Organisation bereits erfüllt sind und welche grundlegenden Sicherheitsanforderungen noch nicht umgesetzt wurden (früher: Basis-Sicherheitscheck).

IT-Notfall

Ein IT-Notfall bezeichnet jede unvorhergesehene Störung, die von dem standardisierten Störungsmanagement, gemäß der vereinbarten Service Levels, in der IT nicht behoben werden kann und die unverzügliche Umsetzung von Maßnahmen erfordert.

IT-Servicemanagement

IT-Servicemanagement (ITSM) bezeichnet die Gesamtheit von Maßnahmen und Methoden, die nötig sind, um die bestmögliche Unterstützung von Geschäftsprozessen durch die IT-Organisation zu erreichen.

IT-Sicherheit

IT-Sicherheit hat den Schutz sämtlicher Informationen, die durch IT-gestützte Systeme verarbeitet werden, als Ziel. Somit wird in der IT-Sicherheit nur das Management der Umsetzung von Maßnahmen für digitale Informationen betrachtet.
IT-Sicherheit und Informationssicherheit sind nicht synonym zu verwenden.

IT-Sicherheitsbeauftragter

Die Bezeichnung IT-Sicherheitsbeauftragter (ITSiBe) betitelt eine Person mit Fachkompetenz für das Management von IT-Sicherheit, die für Aspekte rund um die IT-Sicherheit zuständig ist und sich verantwortlich für das IT-Sicherheitsmanagement zeichnet. Abhängig von der Organisationsform kann eine Unterscheidung zwischen dem ITSiBe und dem ISB getroffen werden.

IT-System

IT-Systeme bezeichnen jegliche Art elektronischer datenverarbeitender Systeme. Typische IT-Systeme sind Großrechner, Server, Clients, Einzelplatz-Computer, Mobiltelefone, Router, Switches und Sicherheitsgateways.

Kategorisierung

Bei der Erhebung des Incident ist anhand definierter Codes eine Kategorisierung vorzunehmen, um ein späteres Controlling zu ermöglichen.

Kern-Absicherung

Der Begriff Kern-Absicherung bezeichnet eine Vorgehensweise des IT-Grundschutz, bei der zunächst besonders gefährdete Geschäftsprozesse und Assets im Fokus stehen.

Key Performance Indicator

Key Performance Indicator (Schlüsselkennzahlen) bezeichnen, bezogen auf den IT-gestützten Geschäftsbetrieb und den Betrieb von Managementsystemen, die Indikatoren für die Ermittlung und Messung der Leistung und Qualität, um die Steuerung spezifischer Zielsetzungen und Zielerfüllungen ermitteln und bewerten sowie daraus ableitend Korrekturmaßnahmen und Verbesserungen einleiten zu können.

Known Error

Ein Known Error (auch bekannter Fehler) ist ein Problem, für das die zugrunde liegende Ursache und ein Workaround dokumentiert wurden. Das Problem Management ist verantwortlich für die Erstellung und Verwaltung von bekannten Fehlern während ihres gesamten Lebenszyklus. Known Error können auch von der Entwicklung oder den Suppliern identifiziert werden.

Konzipierung von Testfällen

Bei der Konzipierung von Testfällen wird geprüft, ob und inwieweit alle geforderten, üblichen Geschäftsvorfälle im Test- und Validierungsmodell abgebildet werden können.

KPI

siehe Key Performance Indicator

kritisches Produkt oder Dienstleistung

Als kritisches Produkt oder Dienstleistung werden die Ressourcen und Kompetenzen der Lieferanten und externen Dienstleister bezeichnet, die zu einer ungewünschten Beeinträchtigung der eigenen Betriebsfähigkeit führen können. Kritische Produkte oder Dienstleistungen müssen im Rahmen der Durchführung von Business Impact Analysen identifiziert und bewertet werden.

Kryptologie

Der Begriff Kryptologie (auch Kryptographie, vom Griechischen kryptós "versteckt" und lógos "Wort") beschreibt in seiner ursprünglichen Bedeutung die Wissenschaft von sicherer, allgemein geheimer, Kommunikation. In der heutigen Nutzung beschreibt der Begriff Kryptologie (mathematische) Konzepte und Verfahren zur Integrität, Authentizität, Vertraulichkeit, Verbindlichkeit.

Kumulationseffekt

Der Kumulationseffekt beschreibt, dass sich der Schutzbedarf eines IT-Systems erhöhen kann, wenn durch Kumulation mehrerer (z. B. kleinerer) Schäden auf einem IT-System ein insgesamt höherer Gesamtschaden entstehen kann. Ein Auslöser kann auch sein, dass mehrere IT-Anwendungen bzw. eine Vielzahl sensitiver Informationen auf einem IT-System verarbeitet werden, sodass durch Kumulation von Schäden der Gesamtschaden höher sein kann.

Löschung

Der Begriff Löschung beschreibt das unwiederbringliche Entfernen von digitalen Daten.

Major Incident

Ein Major Incident beschreibt die höchste Kategorie eines Incident in Bezug auf die Auswirkung. Major Incidents führen zu einer erheblichen Beeinträchtigung der Geschäfts- und Produktionsprozesse.

Malware

Der Begriff Malware wird häufig synonym verwendet zu den Begriffen Schadfunktion, Schadprogramm oder Schadsoftware. Malware ist ein Kunstwort, abgeleitet aus "Malicious Software" und bezeichnet Software, die mit dem Ziel entwickelt wurde, unerwünschte und meistens schädliche Funktionen auszuführen. Zu Malware gehören u. a. Viren, Würmer und Trojaner. Malware ist üblicherweise für eine bestimmte Betriebssystemvariante konzipiert und wird daher meist für verbreitete Systeme und Anwendungen geschrieben.

Managementsystem

Ein Managementsystem verknüpft Methoden, um die definierten Aufgaben des Managements, insbesondere Ziele setzen, steuern und kontrollieren, sowie die Anforderungen an benötigte Prozesse und deren wechselseitiges Zusammenwirken erfolgreich zu erfüllen. Bei der Planung, Einführung, Umsetzung, dem Betrieb, der Überwachung und Überprüfung sowie der Aufrechterhaltung und Verbesserung eines Managementsystems orientieren sich die einschlägigen ISO-Normen am PDCA-Modell.

Maßnahme

siehe Sicherheitsmaßnahme

Maximum-Prinzip

Das Maximum-Prinzip beschreibt, dass der Schaden bzw. die Summe der Schäden mit den schwerwiegendsten Auswirkungen den Schutzbedarf eines Geschäftsprozesses, einer Anwendung bzw. eines IT-Systems bestimmen (im Sinne einer „Vererbung“ des Schutzbedarfs).

Mobiler Datenträger

Mobile Datenträger bezeichnen nicht fest verbaute Speichermedien, die einen ortsungebundenen Datenaustausch oder Datenhaltung ermöglichen.

Mobiles Endgerät

Mobile Endgeräte bezeichnen nicht fest installierte Geräte, die eine ortsungebundene Nutzung eines Geräts ermöglichen.

Modellierung

Der Begriff Modellierung beschreibt bei den Vorgehensweisen nach IT-Grundschutz das Nachbilden des Informationsverbunds einer Organisation mit Hilfe der Bausteine aus dem IT-Grundschutz-Kompendium.

Netzplan

Ein Netzplan stellt eine graphische Übersicht über die Komponenten eines Netzes und ihrer Verbindungen dar.

Netzwerk

Ein Netzwerk bezeichnet allgemein den Zusammenschluss verschiedener technischer, primär selbstständiger elektronischer Systeme, der die Kommunikation der einzelnen Systeme untereinander ermöglicht. Ziel ist hierbei z. B. die gemeinsame Nutzung von Ressourcen wie Netzwerkdruckern, Servern, Dateien und Datenbanken.

Normal Change

Normal Changes folgen dem im Rahmen des Change Management definierten Verfahren und variieren in der Komplexität entsprechend ihrer Priorität, ihren Auswirkungen, ihrer Kategorie und ihres Risikos.

OLA

siehe Operational Level Agreement

Operational Level Agreement

Das Operational Level Agreement (OLA) ist eine Vereinbarung zwischen einem IT Service Provider und einem anderen Teil derselben Organisation. Ein OLA unterstützt die Bereitstellung von IT-Services durch den IT Service Provider für den Kunden und definiert die zu liefernden Waren oder Services sowie die Verantwortlichkeiten der beiden Parteien.

Patch

Ein Patch ist ein Korrekturprogramm, welches Fehler in der Software, wie Sicherheitslücken oder Laufzeitfehler, behebt.

PKI

siehe Public-Key-Infrastruktur

Plan für die Aufrechterhaltung der Betriebsfähigkeit

Ein Plan für die Aufrechterhaltung der Betriebsfähigkeit als Bestandteil des Business Continuity Plan stellt die dokumentierten Informationen für den Wiederanlauf, das Notbetriebsszenario sowie die Wiederherstellung der zu erbringenden Leistung und Qualität eines IT-Service oder Geschäftsprozesses zur Verfügung.

Plausibilitätsprüfung

Im Rahmen einer Plausibilitätsprüfung wird geprüft, ob und inwieweit alle geforderten Ergebnisse und Auswertungen korrekt sind.

Priorisierung

Der Begriff Priorisierung beschreibt im Zusammenhang mit Incident Management die Bestimmung anhand der geschäftskritischen Dringlichkeit und Auswirkung unter Berücksichtigung von Einwirkungen auf den Geschäftsbetrieb, wie Anzahl der betroffenen Kunden, Risiko für Leib und Leben, Compliance-Verstöße oder finanzielle Verluste.

Problem

Ein Problem bezeichnet die Ursache für einen oder mehrere Incidents. Zum Zeitpunkt der Erstellung eines Problem Record ist die Ursache in der Regel unbekannt, für die weitere Untersuchung ist der Problem Management Prozess verantwortlich.

Public-Key-Infrastruktur

Eine Public-Key-Infrastruktur (PKI) bezeichnet ein System, das digitale Zertifikate zur Absicherung rechnergestützter Kommunikation ausstellen, verteilen und prüfen kann.

Release

Ein Release bezeichnet ein oder mehr Changes an einem IT-Service, deren Build, Test und Deployment gemeinsam durchgeführt werden. Ein einzelnes Release kann Changes an Hardware, Software, Dokumentation, Prozessen oder anderen Komponenten enthalten.

Releasetest

Der Begriff Releasetest beschreibt ein Testmodell zum Überprüfen und Testen der planmäßigen Funktionsfähigkeit von Release-Komponenten und Mechanismen vor dem Ausrollen des Releases innerhalb der IT-Abteilung. Das Testmodell stellt beim Release Deployment einen wichtigen Input für den IT-Projektplan dar und enthält unter anderem die erforderlichen Prüfpunkte für die Qualitätssicherung während des Release Deployment sowie detaillierte Skripte für die durchzuführenden Tests.

Release and Deployment Planung

Die Release and Deployment Planung bezeichnet die Erstellung verschiedener Pläne, wobei die Anzahl von verschiedenen Faktoren abhängt. Die Validation erfolgt durch den Abgleich von Service und Release Design mit den Anforderungen.

Release Package

Ein Release Package kann eine einzelne Release Unit oder ein strukturiertes Set von Release Units sein. Die Architektur eines neuen oder veränderten Service bestimmt das Design des Release Package sowie das Vorgehen bei der Planung, Bündelung, Erstellung und dem Test eines Release.

Release Policy

Die Release Policy bezeichnet den Regelsatz für die Überführung unterschiedlicher Arten von Releases in die Live-Betriebsumgebung, wobei zwischen verschiedenen Vorgehensweisen je nach Dringlichkeit und Auswirkung unterschieden wird. Eine Release Policy enthält insbesondere Informationen zu Konventionen zur Release-Identifikation, Anforderungen, Release-Level, Leitlinien für verschiedene Ansätze beim Release Deployment, Einschränkungen für das Release Deployment sowie bevorzugte Mechanismen.

Release Unit

Eine Release Unit beschreibt den Teil eines Service oder einer IT-Infrastruktur, der gemäß der Release Policy der Organisation grundsätzlich gemeinsam releast wird. Release Units variieren nach Typen oder Elementen eines Service Assets oder einer Servicekomponente wie Software und Hardware. Um ein angemessenes Level für Release Units zu bestimmen, wird Folgendes berücksichtigt:

- Die Durchführbarkeit und Zahl der für Release und Deployment notwendigen Changes
- Die Ressourcen und Zeit, die für das Erstellen, Verteilen und Implementieren erforderlich sind
- Die Komplexität der Schnittstellen zwischen der geplanten Unit und den restlichen Services bzw. der IT-Infrastruktur
- Die verfügbaren Kapazitäten in den Erstellungs-, Test-, Verteilungs- und Produktions-Umgebungen

Request for Change

Ein Request for Change bezeichnet den formalen Antrag zur Durchführung eines Change. Er beinhaltet Details zum beantragten Change und kann auf Papier oder elektronisch erfasst werden.

Resilienz

Als Resilienz, im Kontext der Betriebsfähigkeit der IT, ist die Widerstandsfähigkeit des IT-gestützten Geschäftsbetriebs der Organisation zu verstehen sowie die Fähigkeit sich an Änderungen anzupassen, sich auf Bedrohungen einzustellen und mit Beeinträchtigungen des geplanten und vereinbarten IT-Betriebs, zur Zufriedenheit sämtlicher Stakeholder, angemessen umzugehen.

Review

Der Begriff Review bezeichnet die Evaluierung insbesondere eines Change, Problems, Prozesses oder Projekts. Reviews werden grundsätzlich an bestimmten vorher festgelegten Punkten des Lebenszyklus durchgeführt, insbesondere nach dem Abschluss. Zweck eines Reviews ist es sicherzustellen, dass alle Ergebnisse erbracht worden sind, sowie die Identifizierung von Verbesserungsmöglichkeiten.

RfC

siehe Request for Change

Risiko

Ein Risiko bezeichnet die Kombination aus der Eintrittswahrscheinlichkeit, mit der ein Schaden auftritt, und dem Ausmaß dieses Schadens. Hierbei kann eine Konsequenz negativ (Schaden) oder positiv (Chance) sein.

Risikoanalyse

Als Risikoanalyse wird der komplette Prozess bezeichnet, um Risiken zu beurteilen (identifizieren, einschätzen und bewerten) sowie zu behandeln. Risikoanalyse bezeichnet nach den einschlägigen ISO-Normen ISO 31000 und ISO 27005 nur einen Schritt im Rahmen der Risikobeurteilung, die aus den folgenden Schritten besteht:

- Identifikation von Risiken (Risk Identification)
- Analyse von Risiken (Risk Analysis)
- Evaluation oder Bewertung von Risiken (Risk Evaluation)

Risikomanagement

Als Risikomanagement werden alle Aktivitäten mit Bezug auf die strategische und operative Behandlung von Risiken bezeichnet, also alle Tätigkeiten, um Risiken für eine Organisation zu identifizieren, zu steuern und zu kontrollieren.
Die Rahmenbedingungen des operativen Risikomanagements umfassen den Regelprozess aus

- der Identifikation von Risiken,
- der Einschätzung und Bewertung von Risiken,
- der Behandlung von Risiken,
- der Evaluation der Risikoakzeptanz,
- der Überwachung von Risiken und
- der Risikokommunikation.

Rolle

siehe Benutzerrolle

SACM

siehe Service Asset and Configuration Management

Schaden

Schaden bezeichnet in aller Regel jegliche negative Auswirkung für eine Person oder Organisation. Das Ausmaß eines Schadens wird als Schadenshöhe definiert und kann als bezifferbar oder nicht direkt bezifferbar betitelt werden. Die bezifferbaren Schäden können in der Regel mit direkten Aufwänden (z. B. finanzieller Art) dargestellt werden. Zu den nicht direkt bezifferbaren Schäden gehören z. B. Imageschäden oder Reputationsverlust.

Schlüsselkennzahl

Siehe Key Performance Indicator

Schutzbedarf

Der Schutzbedarf bestimmt, welcher Schutz für die Geschäftsprozesse, die dabei verarbeiteten Informationen und die eingesetzte Informations- und Kommunikationstechnik ausreichend und angemessen ist.

Schutzbedarfsfeststellung

Bei einer Schutzbedarfsfeststellung wird der Schutzbedarf der Geschäftsprozesse, der verarbeiteten Informationen, der Anwendungen und der IT-Komponenten bestimmt. Hierbei werden die zu erwartenden Schäden betrachtet, die bei einer Beeinträchtigung der Grundwerte der Informationssicherheit entstehen können.

Schutzziele

siehe Grundwerte

Schwachstelle

Eine Schwachstelle kann ein sicherheitsrelevanter technischer, organisatorischer, personeller oder infrastruktureller Fehler sein. Eine Schwachstelle kann dazu führen, dass eine Gefährdung eintritt und die Organisation oder ein System geschädigt wird.
Ursachen können in der Konzeption, der Implementation, der Konfiguration oder dem Betrieb von Systemen, verwendeten Algorithmen, dem Management von Prozessen oder der Organisation selbst liegen.

Schwachstellenanalyse

Bei einer Schwachstellenanalyse wird geprüft, ob und inwieweit bekannte Schwachstellen weiterhin bestehen.

SCMIS

siehe Supplier and Contract Management Information System

Security Information and Event Management

Ein Security Information and Event Management (SIEM) beschreibt ein System, das die zwei Konzepte Security Information Management und Security Event Management für die Echtzeitanalyse von Sicherheitsmeldungen kombiniert.
Das SIEM ermöglicht es Informationen zu Sicherheitsmeldungen zentral zu sammeln und für eine Bewertung miteinander in Bezug zu setzen.

Server

Als Server wird Soft- oder Hardware bezeichnet, die bestimmte Dienste anderer Soft- oder Hardware (Clients) bereitstellt. Typischerweise wird damit ein Rechner bezeichnet, der beispielsweise seine Funktionalitäten als Applikations-, Daten-, Web- oder E-Mail-Server anderen Rechnern bereitstellt.

Service Asset and Configuration Management

Service Asset and Configuration Management (SACM) beschreibt den Prozess, der sicherstellt, dass die Assets, die für die Erbringung eines Service erforderlich sind, in geeigneter Weise gesteuert werden. Weiterhin stellt der Prozess sicher, dass genaue und zuverlässige Informationen über diese Assets zur Verfügung stehen – wo und wenn sie benötigt werden. Diese Informationen beinhalten Details darüber, wie die Assets konfiguriert wurden sowie die Beziehungen zwischen den Assets.

Service Assets

Als Service Assets gemäß ITIL werden Informationen, Prozesse, Infrastruktur, Anwendungen ebenso angesehen wie Personen, Kapital, Wissen oder die Fähigkeiten des Managements sowie der Organisation.

Service Desk

Der Service Desk ist der Single Point of Contact (SpoC) für die Kommunikation zwischen Service Provider und IT-Anwendern. Ein Service Desk bearbeitet in der Regel Incidents und Service Requests und ist für die Kommunikation mit den IT-Anwendern zuständig.

Service Level Agreement

Ein Service Level Agreement (SLA) beschreibt eine Vereinbarung zwischen einem IT Service Provider und einem Kunden. Das SLA beschreibt den beschreibt den jeweiligen IT-Service, dokumentiert Service Level Ziele und legt die Verantwortlichkeiten des IT Service Providers und des Kunden fest. Ein einzelnes SLA kann mehrere IT-Services oder mehrere Kunden abdecken.

Sicherheitsanforderung

Die Sicherheitsanforderungen definieren das zu avisierende Sicherheitsniveau und bestimmen den Grad sowie die Güte der umzusetzenden Maßnahmen, um den definierten Anforderungen an die Informationssicherheit gerecht zu werden.

Sicherheitskonzept

Ein Sicherheitskonzept dient zur Umsetzung der Sicherheitsstrategie und beschreibt die geplante Vorgehensweise, um die gesetzten Sicherheitsziele einer Organisation zu erreichen.
Das Sicherheitskonzept ist das zentrale Dokument im Sicherheitsprozess, durch das sich die umzusetzenden Sicherheitsmaßnahmen definieren.

Sicherheitskonzeption

Die Erstellung einer Sicherheitskonzeption ist eine der zentralen Aufgaben des Informationssicherheitsmanagements. Aufbauend auf den Ergebnissen von Strukturanalyse und Schutzbedarfsfeststellung werden hier die erforderlichen Sicherheitsmaßnahmen identifiziert und im Sicherheitskonzept dokumentiert.

Sicherheitsmaßnahme

Mit Sicherheitsmaßnahme, auch Maßnahme, werden alle Aktivitäten bezeichnet, die dazu dienen Sicherheitsanforderungen gerecht zu werden. Hierzu zählen insbesondere technische und organisatorische, als auch personelle und infrastrukturelle Sicherheitsmaßnahmen.

SIEM

siehe Security Information and Event Management

Single Point of Contact

Als Single Point of Contact (SpoC) wird in einer Organisation eine zentrale, einzig mögliche, Anlaufstelle für ein bestimmtes Thema, oftmals als Kontakt für den Support der IT-Anwender über den Service Desk, bezeichnet.

SLA

siehe Service Level Agreement

SPoC

siehe Single Point of Contact

Standard-Absicherung

Der Begriff Standard-Absicherung bezeichnet eine Vorgehensweise des IT-Grundschutz zur Implementierung eines kompletten Sicherheitsprozesses, um eine Organisation sowohl umfassend als auch in der Tiefe abzusichern.

Standard-Change

Ein Standard-Change ist ein vorab genehmigter Change, der von geringem Risiko ist, relativ häufig eingesetzt wird und einem bestimmten Verfahren oder einer Arbeitsanweisung folgt, wie die Zurücksetzung eines Passworts oder die Bereitstellung der Grundausstattung für einen neuen Mitarbeiter. Für die Implementierung eines Standard-Change ist kein Request for Change (RfC) erforderlich, sondern wird über andere Mechanismen erfasst und verfolgt, etwa über einen Service Request.

Störung

siehe Beeinträchtigung

Strukturanalyse

Die Strukturanalyse beschreibt das schrittweise Vorgehen zur Erhebung und Darstellung der Informationen über den definierten Informationsverbund. Zentrale Informationen, die erhoben werden müssen, sind die Geschäftsprozesse, Anwendungen, IT-Systeme, Netze, Räume, Gebäude und Verbindungen.

Supplier

Ein Supplier ist eine Drittpartei, die für die Bereitstellung von Waren oder Services verantwortlich ist, welche für die Erbringung von IT-Services benötigt werden. Zu den Suppliern zählen u. a. Hardware- und Softwareanbieter, Netzwerk- und Telekommunikationsanbieter oder Outsourcing-Organisationen.

Supplier and Contract Management Information System

Das Supplier and Contract Management Information System (SCMIS) ist eine Kombination von Tools, Daten und Informationen, die zur Unterstützung des Supplier Management genutzt werden.

Supplier Management

Das Supplier Management ist ein Prozess, der sicherstellen soll, dass Supplier ein positives Kosten-Nutzen-Verhältnis liefern, dass alle Verträge mit Suppliern die Anforderungen der Organisation unterstützen und alle Supplier ihre vertraglichen Verpflichtungen erfüllen.

System

Wird oft als verallgemeinernder Begriff für „Services, Hardware, Software, Infrastruktur-Komponenten oder technischen Schnittstellen“ verwendet. Siehe auch IT-System.

Test- und Validierungskonzept

Ein Test- und Validierungskonzept beschreibt die Spezifikationen zur Durchführung, Überwachung sowie Aufrechterhaltung und Verbesserung eines Test- und Validierungsmodells.

Test- und Validierungsmodell

Ein Test- und Validierungsmodell dient der Qualitätssicherung von IT-Services in Bezug auf die zwischen den Vertragsparteien vereinbarten Fähigkeiten, Ressourcen und Kapazitäten. Bei der Planung eines Test- und Validierungsmodells werden interne und externe IT-Services berücksichtigt. Test- und Validierungsmodelle sind fester Bestandteil des Release- und Deployment Management Prozesses und liefern Ergebnisse, die vom Change Evaluation Prozess bearbeitet werden.

Test- und Validierungsphase

Eine Test- und Validierungsphase beschreibt einen sachlich und zeitlich in sich geschlossenen Abschnitt eines Testmodells, in dem für relevante IT-Services definierte Testaufgaben durchgeführt werden.

UC

siehe Underpinning Contract

Underpinning Contract

Der Underpinning Contract ist ein Vertrag zwischen einem IT Service Provider und einer Drittpartei. Die Drittpartei stellt Waren oder Services zur Verfügung, die die Bereitstellung eines IT-Service für einen Kunden unterstützen. Der Underpinning Contract definiert Ziele und Verantwortlichkeiten, um die in einem oder mehreren Service Level Agreements vereinbarten Service Level Ziele zu erreichen.

Verbindlichkeit

Unter Verbindlichkeit werden die Sicherheitsziele Authentizität und Nichtabstreitbarkeit zusammengefasst. Bei der Übertragung von Informationen bedeutet dies, dass die Informationsquelle ihre Identität bewiesen hat und der Empfang der Nachricht nicht in Abrede gestellt werden kann.

Verfügbarkeit

Die Verfügbarkeit von Daten bestimmt die Bereitstellung der Daten zu definierten Zeitpunkten im definierten Umfang.

Verteilungseffekt

Der Verteilungseffekt kann sich auf den Schutzbedarf relativierend auswirken, wenn eine Anwendung einen hohen Schutzbedarf besitzt, ihn aber nicht auf ein betrachtetes IT-System überträgt, weil auf diesem IT-System nur unwesentliche Teilbereiche der Anwendung laufen.

Vertraulichkeit

Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.

Virus

Der Begriff Virus beschreibt eine klassische Form von Schadsoftware, die sich selbst verbreitet und unterschiedliches Schadpotenzial in sich tragen kann, von keinerlei Schadfunktion bis hin zum Löschen der Daten auf einer Festplatte. Viren treten in Kombination mit einem Wirt auf, z. B. einem infizierten Dokument oder Programm.

Vollständigkeitsprüfung

Bei einer Vollständigkeitsprüfung wird geprüft, ob und inwieweit alle geforderten Daten, Schnittstellen und Funktionen eines IT-Services implementiert bzw. vorhanden sind und die definierten Funktionen ordnungsgemäß erbracht werden.

Workaround

Ein Workaround (auch Umgehungslösung) beschreibt die Reduzierung oder Beseitigung der Auswirkungen von Incidents oder Problemen, für die noch keine vollständige Lösung verfügbar sind, z. B. durch den Neustart eines ausgefallenen Configuration Item. Workarounds für Probleme werden in Known Error Records dokumentiert. Workarounds für Incidents, die nicht über zugeordnete Problem Records verfügen, werden in Incident Records dokumentiert.

Zugang

Mit Zugang wird die Berechtigungsaktivität für die Nutzung von Netzwerken, IT-Systemen und System-Komponenten bezeichnet.

Zugriff

Mit Zugriff wird die Berechtigungsaktivität für die Nutzung von Informationen und Daten bezeichnet.

Zutritt

Mit Zutritt wird das Betreten von abgegrenzten Bereichen wie z. B. Räumen, Gebäuden oder geschützten Arealen auf einem Gelände bezeichnet.

Zwischenfall

siehe Beeinträchtigung