

DIN EN ISO/IEC 27041

ICS 35.040

Einsprüche bis 2016-04-26

Entwurf

**Informationstechnik –
IT-Sicherheitsverfahren –
Leitfaden zur Sicherung der Tauglichkeit und Eignung von
Vorfall-Untersuchungsmethoden (ISO/IEC 27041:2015);
Deutsche und Englische Fassung FprEN ISO/IEC 27041:2016**

Information technology –
Security techniques –
Guidance on assuring suitability and adequacy of incident investigative method
(ISO/IEC 27041:2015);
German and English version FprEN ISO/IEC 27041:2016

Technologies de l'information –
Techniques de sécurité –
Directives sur la façon d'assurer l'aptitude à l'emploi et l'adéquation d'une méthode
d'investigation d'incident (ISO/IEC 27041:2015);
Version allemande et anglaise FprEN ISO/IEC 27041:2016

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2016-02-26 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfes besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal des DIN unter www.entwuerfe.din.de bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an nia@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/stellungnahme oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Informationstechnik und Anwendungen (NIA), 10772 Berlin (Hausanschrift: Burggrafenstr. 6, 10787 Berlin).

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 58 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales Vorwort

Dieses Dokument (FprEN ISO/IEC 27041:2016) wurde vom Technischen Komitee ISO/IEC JTC 1/SC 27 „IT Security techniques“ erarbeitet, dessen Sekretariat vom DIN (Deutschland) gehalten wird. Auf Grundlage eines CEN/BT Beschlusses wurde ISO/IEC 27041:2015 im einstufigen Annahmeverfahren (UAP) als FprEN ISO/IEC 27041:2016 ohne Abänderung übernommen.

Das zuständige deutsche Spiegelgremium ist der Arbeitskreis NA 043-01-27-04 AK „IT-Sicherheitsmaßnahmen und Dienste“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung der FprEN ISO/IEC 27041 beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen Text.

**Informationstechnik — IT-Sicherheitsverfahren — Leitfaden zur Sicherung
der Tauglichkeit und Eignung von Vorfall-Untersuchungsmethoden
(ISO/IEC 27041:2015)**

Technologies de l'information — Techniques de sécurité — Directives sur la façon d'assurer l'aptitude à l'emploi et l'adéquation d'une méthode d'investigation d'incident (ISO/IEC 27041:2015)

Information technology — Security techniques — Guidance on assuring suitability and adequacy of incident investigative method (ISO/IEC 27041:2015)

ICS:

Deskriptoren

Dokument-Typ: Europäische Norm
Dokument-Untertyp:
Dokument-Stage: Einstufiges Annahmeverfahren
Dokument-Sprache: D

STD Version 2.7g

Inhalt

	Seite
Europäisches Vorwort	4
Vorwort	5
Einleitung	6
1 Anwendungsbereich	11
2 Normative Verweisungen	11
3 Begriffe	11
4 Symbole und Abkürzungen	14
5 Entwicklung von Methoden und deren Sicherung	14
5.1 Überblick	14
5.2 Allgemeine Grundsätze	15
5.3 Allgemeines Entwicklungs- und Einsatzmodell	15
5.4 Sicherungsstufen	16
5.5 Erfassung und Analyse von Anforderungen	16
5.5.1 Allgemeine Grundsätze der Anforderungen	16
5.5.2 Funktionale Anforderungen	18
5.5.3 Verifizierung von Anforderungen	18
5.6 Prozessgestaltung	18
5.6.1 Überblick	18
5.6.2 Auswahl des Tools	18
5.6.3 Unsicherheit und Risikobewertung	18
5.7 Prozessverwirklichung	19
5.7.1 Überblick	19
5.7.2 Auswahl des Tools — Hinweise für den Einsatz	19
5.8 Prozessverifizierung	20
5.8.1 Allgemeine Grundsätze der Verifizierung	20
5.8.2 Verifizierung von Prozessen	20
5.8.3 Verifizierung von Tools	20
5.9 Prozessvalidierung	20
5.9.1 Allgemeine Grundsätze der Validierung	20
5.9.2 Umfassende Validierung	21
5.9.3 Ausreichende Validierung	21
5.9.4 Vollständig validierte Prozesse	21
5.9.5 Nicht bestandene Validierung	21
5.10 Bestätigung	22
5.11 Einsatz	22
5.11.1 Auswahl der Tools	22
5.12 Überprüfung und Aufrechterhaltung	22
6 Sicherungsmodelle	22
6.1 Überblick	22
6.2 Interne Sicherung	23
6.3 Externe Sicherung	23
6.4 Kombinierte Sicherung	23
7 Erstellung von Sicherungsnachweisen	23
7.1 Überblick	23

7.2	Vorbereitung der Validierung	24
7.3	Erstellen von Validierungsnachweisen	24
7.4	Aufrechterhaltung der Validierung	24
7.5	Validierung von Untersuchungen	25
7.6	Validierung von Ermittlungen	25
Anhang A (informativ) Beispiele		26
A.1	Arbeitsanweisung	26
A.2	Validierungsplan	28
A.3	Validierungsnachweis	30
A.4	Aussage zur Bestätigung	31
Literaturhinweise		32

Europäisches Vorwort

Der Text von ISO/IEC 27041:2015 wurde vom Technischen Komitee ISO/IEC JTC/TC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) und der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und auf Grundlage eines CEN/BT Beschlusses als FprEN ISO/IEC 27041:2016 übernommen.

Dieses Dokument ist derzeit zum einstufigen Annahmeverfahren vorgelegt.

Anerkennungsnotiz

Der Text von ISO/IEC 27041:2015 wurde vom CEN als FprEN ISO/IEC 27041:2016 ohne irgendeine Abänderung genehmigt.

Vorwort

ISO (die Internationale Organisation für Normung) und IEC (die Internationale Elektrotechnische Kommission) bilden das auf die weltweite Normung spezialisierte System. Nationale Normungsorganisationen, die Mitglieder von ISO oder IEC sind, beteiligen sich an der Entwicklung von Internationalen Normen in Technischen Komitees, die von der jeweiligen Organisation eingerichtet wurden, um spezifische Gebiete technischer Aktivitäten zu behandeln. Auf Gebieten von beiderseitigem Interesse arbeiten die Technischen Komitees von ISO und IEC zusammen. Internationale Organisationen, staatlich und nicht-staatlich, in Liaison mit ISO und IEC, nehmen ebenfalls an der Arbeit teil. Auf dem Gebiet der Informationstechnologie haben ISO und IEC ein gemeinsames technisches Komitee (JTC, en: joint technical committee), ISO/IEC JTC 1, eingerichtet.

Die Verfahren, die bei der Entwicklung dieses Dokuments angewendet wurden und die für die weitere Pflege vorgesehen sind, werden in den ISO/IEC-Direktiven, Teil 1 beschrieben. Im Besonderen sollten die für die verschiedenen ISO-Dokumentenarten notwendigen Annahmekriterien beachtet werden. Dieses Dokument wurde in Übereinstimmung mit den Gestaltungsregeln der ISO/IEC-Direktiven, Teil 2 erarbeitet (siehe www.iso.org/directives).

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren. Details zu allen während der Entwicklung des Dokuments identifizierten Patentrechten finden sich in der Einleitung und/oder in der ISO-Liste der empfangenen Patenterklärungen (siehe www.iso.org/patents).

Jeder in diesem Dokument verwendete Handelsname wird als Information zum Nutzen der Anwender angegeben und stellt keine Anerkennung dar.

Eine Erläuterung der Bedeutung ISO-spezifischer Benennungen und Ausdrücke, die sich auf Konformitätsbewertung beziehen, sowie Informationen über die Beachtung der WTO-Grundsätze zu technischen Handelshemmnissen (TBT, en: Technical Barriers to Trade) durch ISO enthält der folgende Link: Foreword — Supplementary information.

Das für dieses Dokument verantwortliche Komitee ist ISO/IEC JTC 1, *Information technology*, SC 27, *IT Security techniques*.

Einleitung

Über diese Internationale Norm

Diese Internationale Norm beschäftigt sich damit zu sichern, dass der eingesetzte Ermittlungsprozess für den zu ermittelnden Vorfall und die geforderten Ergebnisse geeignet ist. Sie beschreibt außerdem auf abstrakter Ebene das Konzept des scheinbaren Aufspaltens komplexer Prozesse in eine Reihe kleinerer, unteilbarer Teilprozesse, die bei der Entwicklung von einfachen aber dennoch widerstandsfähigen Ermittlungsmethoden behilflich sind. Sie sollte von jeder Person berücksichtigt werden, die eine Ermittlung genehmigt, sie anleitet, sie lenkt oder durchführt. Sie sollte vor jeder Ermittlung bezüglich der Grundsätze und Prozesse (definiert in ISO/IEC 27043:2015) und der ordnungsgemäßen Vorbereitung und Planung (definiert in ISO/IEC 27035-2¹⁾) angewendet werden, um sicherzustellen, dass die Methoden zur Einbindung in die Ermittlungsprozesse nach ISO/IEC 27037:2012 und ISO/IEC 27042:2015 geeignet sind.

Zusammenhang mit anderen Normen

Diese Internationale Norm ist dafür vorgesehen, andere Normen und Dokumente, die Leitfäden für die Ermittlung von und für die Vorbereitung von Vorfall-Ermittlungen in der Informationssicherheit enthalten, zu ergänzen. Sie stellt keinen allumfassenden Leitfaden dar, sondern legt bestimmte wesentliche Grundsätze fest, die sicherstellen sollen, dass die richtigen Tools, Techniken und Methoden ausgewählt werden können und dass deren Zweckdienlichkeit bei Bedarf nachgewiesen werden kann.

Zweck dieser Internationalen Norm ist es außerdem, Entscheidungsträger, die die Glaubwürdigkeit der ihnen vorgelegten digitalen Beweismittel feststellen müssen, mit Informationen zu versorgen. Sie gilt für Organisationen, die potentielle digitale Beweismittel schützen, analysieren und vorlegen müssen. Sie ist für richtungsweisende Stellen von Bedeutung, die Verfahren zur digitalen Beweisführung erstellen und auswerten, und die häufig Teil einer größeren Stelle zur Beweisführung sind.

Diese Internationale Norm beschreibt einen Teil eines umfassenden Ermittlungsprozesses, der neben anderen die folgenden Themenbereiche umfasst:

- Handhabung von Vorfällen, einschließlich der Vorbereitung und Planung von Ermittlungen;
- Umgang mit digitalen Beweismitteln;
- Einsatz von Schwärzung und damit verbundene Probleme;
- Angriffspräventions- und -erkennungssysteme, einschließlich Informationen, die aus diesen Systemen erlangt werden können;
- Sicherheit der Speicherung, einschließlich Löschen von Daten auf temporär belegten Speichermedien (en: sanitization);
- Sicherstellen, dass Ermittlungsmethoden zweckdienlich sind;
- Durchführen von Analysen und Interpretation digitaler Beweismittel;
- Verstehen von Grundsätzen und Prozessen bei der Ermittlung von digitalen Beweismitteln;

1) In Veröffentlichung.

- Management von Sicherheitsvorfällen, einschließlich der Herleitung von Beweismitteln aus den am Management von Sicherheitsvorfällen beteiligten Systemen;
- Zusammenhang zwischen elektronischen Beweissicherungstechniken und anderen Ermittlungsmethoden, sowie der Einsatz von elektronischen Beweissicherungstechniken in anderen Ermittlungen;
- Steuerung von Ermittlungen, einschließlich forensischer Ermittlungen.

Diese Themenbereiche werden zum Teil von folgenden ISO/IEC-Normen behandelt:

- ISO/IEC 27037:2012

Diese Internationale Norm beschreibt die Mittel, mit denen die Beteiligten der Anfangsphase einer Ermittlung, einschließlich der ersten Reaktion, versichern können, dass ausreichend potentielle digitale Beweismittel gesammelt wurden, um die Ermittlung angemessen durchzuführen.

- ISO/IEC 27038:2014

Manche Dokumente können Informationen enthalten, die einigen Gemeinschaften nicht offen zugänglich gemacht werden dürfen. Modifizierte Dokumente können für diese Gemeinschaften freigegeben werden, nachdem eine angemessene Bearbeitung des Originaldokuments erfolgt ist. Das Entfernen von Informationen, die nicht freigegeben werden dürfen, wird als „Schwärzen“ bezeichnet.

Das digitale Schwärzen von Dokumenten ist ein relativ neuer Bereich des Dokumentenmanagements, der besondere Fragen und potentielle Risiken aufwirft. Wenn digitale Dokumente geschwärzt werden, dürfen die entfernten Informationen nicht wiederherstellbar sein. Demzufolge ist darauf zu achten, dass geschwärzte Informationen dauerhaft aus dem digitalen Dokument entfernt werden (z. B. dürfen sie nicht nur in nicht darstellbaren Teilen des Dokuments ausgeblendet werden).

ISO/IEC 27038:2014 legt Methoden für das digitale Schwärzen von digitalen Dokumenten fest. Darüber hinaus legt sie Anforderungen an die Software fest, die für das Schwärzen verwendet werden kann.

- ISO/IEC 27040:2015

Diese Internationale Norm liefert ausführliche technische Leitlinien darüber, wie Organisationen ein angemessenes Maß an Risikominderung festlegen können, indem sie einen bewährten und konsistenten Ansatz bei der Planung, Gestaltung, Dokumentation und Umsetzung der Datenspeichersicherheit anwenden. Die Speichersicherheit bezieht sich auf den Schutz (Sicherheit) von Informationen an deren Speicherort, und auf die Sicherheit der Informationen bei der Übertragung über die Kommunikationsschnittstellen in Verbindung mit der Speicherung. Die Speichersicherheit umfasst die Sicherheit von Geräten und Medien, die Sicherheit von Managementaktivitäten im Zusammenhang mit Geräten und Medien, die Sicherheit von Anwendungen und Diensten, und die für die Endanwender während der Lebensdauer von Geräten und Medien und nach deren Lebensdauer relevante Sicherheit.

Durch das Einbringen von Verschleierungsfunktionen können Sicherheitsfunktionen, wie Verschlüsselung und das Löschen von Daten auf temporär belegten Speichermedien, die Fähigkeit zur Ermittlung beeinflussen. Sie müssen vor und während der Durchführung einer Ermittlung berücksichtigt werden. Sie können auch wichtig sein bei der Sicherstellung, dass die Speicherung von Beweismitteln während und nach einer Ermittlung angemessen vorgenommen und gesichert wird.

- ISO/IEC 27042:2015

Diese Internationale Norm beschreibt die Art und Weise, wie die während einer Ermittlung anzuwendenden Methoden und Prozesse ausgelegt und verwirklicht werden können, um eine korrekte Bewertung von potentiellen digitalen Beweismitteln, eine Interpretation von digitalen Beweismitteln und eine effektive Berichterstattung über die Feststellungen zu ermöglichen.

— ISO/IEC 27043:2015

Diese Internationale Norm legt die üblicherweise wichtigsten Grundsätze und Prozesse fest, die der Ermittlung von Vorfällen zugrunde liegen, und enthält ein Rahmenmodell für alle Stufen der Ermittlung.

Die folgenden ISO/IEC-Projekte behandeln zum Teil ebenfalls die vorstehend festgelegten Themenbereiche und können als einschlägige Normen zu einem bestimmten Zeitpunkt nach der Veröffentlichung dieser Norm veröffentlicht werden.

— ISO/IEC 27035 (alle Teile)²⁾

Diese Normenreihe besteht aus drei Teilen, die einen strukturierten und geplanten Ansatz für Organisationen für das Management von Sicherheitsvorfällen enthalten. Diese Teile sind:

— ISO/IEC 27035-1³⁾

Dieser Teil enthält die Grundlagen und Phasen des Managements von Informationssicherheitsvorfällen. Er vereint diese Grundlagen mit den Grundsätzen in einem strukturierten Ansatz zur Erkennung von, Berichterstattung von, Beurteilung von, Reaktion auf und Nutzung von Erfahrungen.

— ISO/IEC 27035-2⁴⁾

Dieser Teil enthält die Grundlagen für die Planung und Vorbereitung von Reaktionen auf einen Vorfall. Die Grundlagen, einschließlich Vorfallmanagementpolitik und -plan, Zusammenstellung eines Teams zur Reaktion auf einen Vorfall sowie Unterweisungen und Sensibilisierungen, basieren auf der Planungs- und Vorbereitungsphase des in ISO/IEC 27035-1⁵⁾ dargestellten Modells. Dieser Teil behandelt außerdem die Phase „Gewinnung von Erkenntnissen“ des Modells.

— ISO/IEC 27035-3⁶⁾

Dieser Teil enthält die Verantwortlichkeiten des Personals und praktische Tätigkeiten zur Reaktion auf einen Vorfall innerhalb der Organisation. Ein besonderes Augenmerk wird dabei auf die Tätigkeiten des Teams zur Reaktion auf einen Vorfall gelegt, z. B. Tätigkeiten zur Überwachung, Erkennung, Analyse und Reaktion im Zusammenhang mit den erfassten Daten oder Sicherheitsereignisse.

2) In Veröffentlichung.

3) In Veröffentlichung.

4) In Veröffentlichung.

5) In Veröffentlichung.

6) In Veröffentlichung.

— ISO/IEC 27050 (alle Teile)⁷⁾

Dieses Dokument behandelt Tätigkeiten der elektronischen Beweissicherung, einschließlich unter anderem der Identifizierung, des Erhalts, der Erfassung, der Verarbeitung, der Überprüfung, der Analyse und der Erstellung von elektronisch gespeicherten Informationen (ESI, en: electronically stored information). Außerdem liefert es Leitlinien zu Maßnahmen, die von der ersten Erstellung von ESI bis hin zu deren Verteilung reichen, mit denen eine Organisation ein Risiko mindern und Ausgaben verringern kann, falls die elektronische Beweissicherung relevant werden sollte. Es ist sowohl für technisches Personal als auch für nichttechnisches Personal relevant, das an einigen oder an allen Tätigkeiten der elektronischen Beweissicherung beteiligt ist. Es ist wichtig anzumerken, dass dieser Leitfaden nicht dafür vorgesehen ist, lokalen Gesetzen und Verordnungen zu widersprechen oder sie zu ersetzen.

Die elektronische Beweissicherung dient häufig als Einflussfaktor für Ermittlungen, sowie auch für Beweissuch- und Beweisaufnahmetätigkeiten. Des Weiteren müssen die Empfindlichkeit und die Kritikalität der Daten manchmal besonders geschützt werden, wie z. B. durch die Speichersicherheit zum Schutz vor der Verletzung der Datensicherheit.

— ISO/IEC 30121:2015

Diese Internationale Norm liefert einen Rahmen für Steuerungsgremien von Organisationen (einschließlich der Inhaber, Vorstände, Direktoren, Partner, leitende Angestellte oder ähnliche Personen), um eine Organisation am besten auf digitale Nachforschungen vorzubereiten. Diese Internationale Norm gilt für die Entwicklung von strategischen Prozessen (und Entscheidungen) im Zusammenhang mit der Rückhaltung, Verfügbarkeit, Zugänglichkeit und Wirtschaftlichkeit von digitalen Beweismitteln. Diese Internationale Norm gilt für alle Arten und Größen von Organisationen. Die Internationale Norm behandelt die vorausschauende strategische Vorbereitung von digitalen Ermittlungen durch eine Organisation. Die forensische Bereitschaft versichert, dass eine Organisation geeignete und maßgebliche strategische Vorbereitungen getroffen hat, um potentielle beweiskräftige Ereignisse zu behandeln. Infolge einer unvermeidbaren Verletzung der Datensicherheit, Betrug und Rufschädigung können Maßnahmen eingeleitet werden. In jeder Situation muss die Informationstechnologie (IT) strategisch eingesetzt werden, um die effektive Verfügbarkeit, Zugänglichkeit und Wirtschaftlichkeit der Beweismittel zu maximieren.

Bild 1 zeigt typische Tätigkeiten, die bei einem Vorfall und dessen Ermittlung eine Rolle spielen. Die im Bild dargestellten Zahlen (z. B. 27037) weisen auf eine der vorstehend aufgelisteten Internationalen Normen hin, und schattierte Balken geben an, wo sie jeweils mit hoher Wahrscheinlichkeit direkt angewendet werden können oder Einfluss auf den Ermittlungsprozess besitzen (z. B. durch Festlegen von Regeln oder Beschränkungen). Es wird dennoch empfohlen, alle Dokumente vor und während der Planungs- und Vorbereitungsphasen hinzuzuziehen. Die dargestellten Prozessklassen werden in dieser Norm umfassend definiert und die festgestellten Tätigkeiten stimmen mit denen in ISO/IEC 27035-2 und ISO/IEC 27037 näher erläuterten Tätigkeiten überein.

7) In Veröffentlichung.

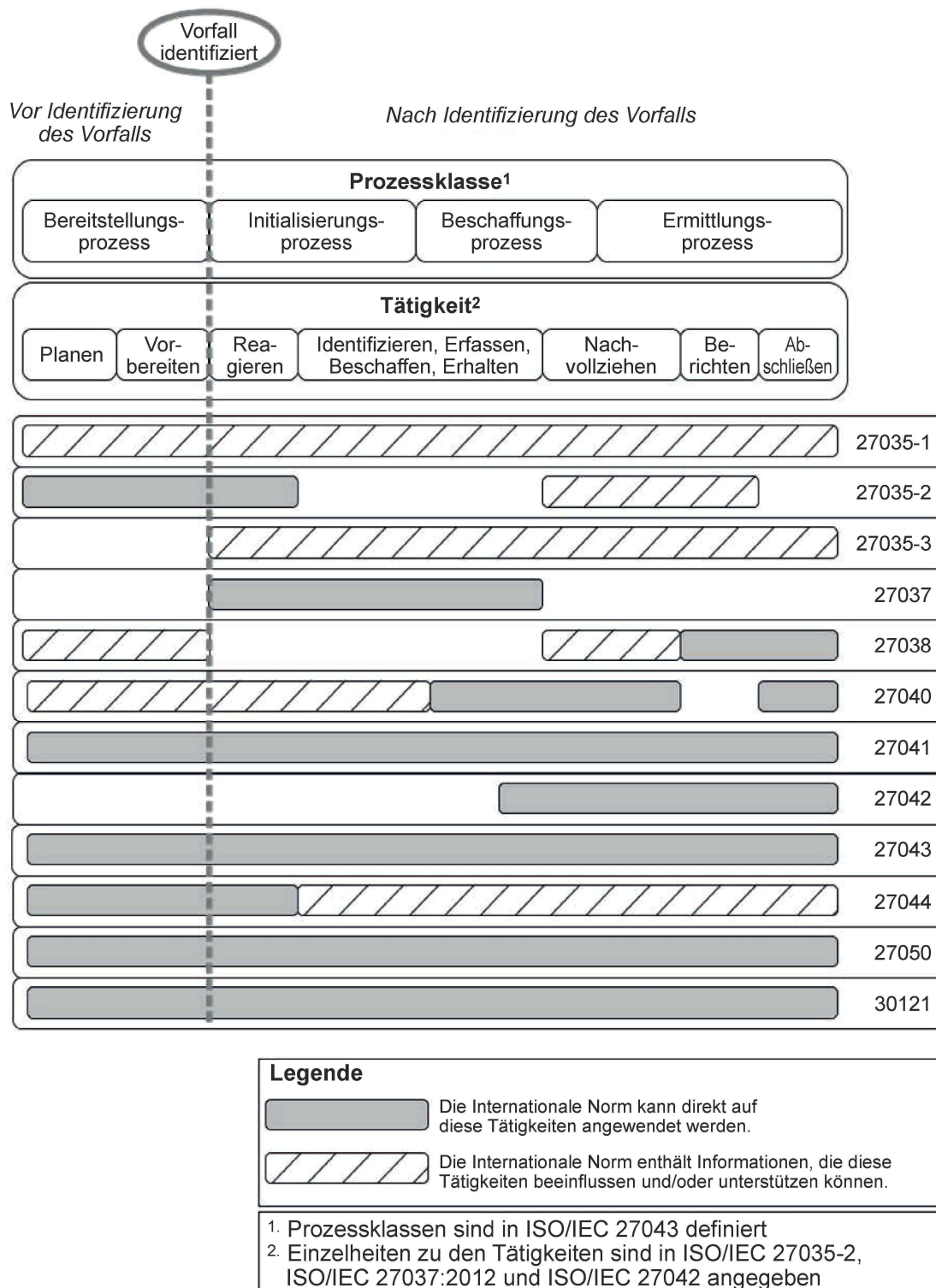


Bild 1 — Anwendbarkeit der Normen auf die Ermittlungsprozessklassen und Ermittlungstätigkeiten

1 Anwendungsbereich

Diese Internationale Norm liefert einen Leitfaden für die Instrumente, mit denen zugesichert wird, dass die eingesetzten Vorfall-Untersuchungsmethoden und -prozesse im Bereich der Informationssicherheit „zweckdienlich“ sind. Sie umfasst bewährte Verfahrensweisen zur Festlegung von Anforderungen, Beschreibung von Methoden und Bereitstellung von Nachweisen, mit denen aufgezeigt werden kann, dass die Durchführung dieser Methoden den Anforderungen entspricht. Sie betrachtet, wie Anbieter- und Drittparteien-Prüfungen eingesetzt werden können, um diese Sicherungsprozesse zu unterstützen.

Ziel dieses Dokuments ist,

- einen Leitfaden für die Erfassung und Analyse von funktionalen und nicht funktionalen Anforderungen im Zusammenhang mit einer Vorfallermittlung im Bereich Informationssicherheit (IS) zu liefern;
- einen Leitfaden für den Einsatz der Validierung als Hilfsmittel zur Eignungssicherung von Prozessen, die an der Ermittlung beteiligt sind, zu bieten;
- einen Leitfaden für die Beurteilung der geforderten Validierungsebenen und den für die Durchführung der Validierung geforderten Nachweis zu liefern;
- einen Leitfaden für die Einbindung externer Prüfungen und Dokumentationen in den Validierungsprozess zu bieten.

2 Normative Verweisungen

Die folgenden Dokumente, die in diesem Dokument teilweise oder als Ganzes zitiert werden, sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

ISO/IEC 27000:2013, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO/IEC 27000:2013 und die folgenden Begriffe.

3.1

unteilbar

durchführen von nur einer einzelnen Funktion

Anmerkung 1 zum Begriff: Eine *Methode* (3.11) zur Wiederherstellung aller Echtzeitdateien eines Geräts kann unteilbar sein, wenn sie ausschließlich auf dem Einsatz von Metadaten des Dateisystems basiert. Eine Methode zur Wiederherstellung aller gelöschten Dateien ist wahrscheinlich nicht unteilbar, da sie Teilmethoden benötigt, mit denen bestimmte Dateistrukturen der Daten auf dem Speichermedium basierend auf dem Wissen über die Dateiinhalte (z. B. .jpg, .png, .odt, XML usw.) identifiziert und extrahiert werden.

3.2

Black-Box-Test

untersuchen eines Prozesses, indem er zur Verarbeitung bekannter Eingaben angewendet wird und die Ergebnisse anschließend mit vorhergesagten Ausgaben, die die Anforderungen an den Prozess darstellen, verglichen werden

3.3

Auftraggeber

natürliche oder juristische Person, in deren Namen die Ermittlung durchgeführt werden soll

[QUELLE: ISO/IEC 27042:2015, 3.2]

3.4

Bestätigung

formale Beurteilung des vorliegenden objektiven Nachweises, dass ein Prozess für einen bestimmten Zweck geeignet ist (oder weiterhin geeignet bleibt)

3.5

zeitgleiche Notizen

zeitgleiche Aufzeichnungen

schriftliche Aufzeichnungen über durchgeführte Tätigkeiten und getroffene Entscheidungen, die erstellt werden, während die Tätigkeiten durchgeführt und die Entscheidungen getroffen werden, oder im Anschluss daran, sobald dies praktisch möglich ist

Anmerkung 1 zum Begriff: In vielen Zuständigkeitsbereichen wird gefordert, dass zeitgleiche Notizen handschriftlich mit nicht löschbarer Tinte in einem manipulationssicheren Notizbuch angefertigt werden, um in Fragen der Nicht-abstreitbarkeit und Zulässigkeit Hilfestellung zu leisten.

[QUELLE: ISO/IEC 27042:2015, 3.4]

3.6

Untersuchung

Reihe von Prozessen, die durchgeführt werden, um relevante potentielle digitale Beweismittel aus einer oder mehreren Quellen zu identifizieren und wiederherzustellen

[QUELLE: ISO/IEC 27042:2015, 3.7]

3.7

Ermittlung

Durchführung von *Untersuchungen* (3.6), Analysen und Interpretationen für ein besseres Verständnis des Vorfalls

[QUELLE: ISO/IEC 27042:2015, 3.10]

3.8

Leiter der Ermittlungsgruppe

Person, die die Ermittlungen auf strategischer Ebene anführt

[QUELLE: ISO/IEC 27042:2015, 3.11]

3.9

Ermittlungsgruppe

alle Personen, die direkt an der Durchführung der Ermittlung beteiligt sind

[QUELLE: ISO/IEC 27042:2015, 3.12]

3.10

Ermittler

Mitglied der *Ermittlungsgruppe* (3.9), einschließlich des *Leiters der Ermittlungsgruppe* (3.8)

[QUELLE: ISO/IEC 27042:2015, 3.13]

3.11

Methode

Definition eines Arbeitsablaufs, der eingesetzt werden kann, um aus festgelegten Eingaben Daten zu erzeugen oder Informationen herzuleiten, die das Ergebnis darstellen

Anmerkung 1 zum Begriff: Im Idealfall sollte eine *Methode* (3.11) *unteilbar* (3.1) sein (d. h. sie sollte nicht mehr als eine Funktion umfassen), um den erneuten Einsatz von Methoden und der davon abgeleiteten *Prozesse* (3.12) zu ermöglichen und den für die Validierung von Prozessen erforderlichen Arbeitsaufwand zu verringern.

3.12

Prozess

einsatzbezogene Umsetzung einer *Methode* (3.11)

3.13

Hersteller

Ersteller oder Anbieter eines *Tools* (3.17), einschließlich jeder Person, die ein Tool modifiziert oder anpasst

Anmerkung 1 zum Begriff: Die Person(en) oder die Organisation(en), die für die Erstellung oder Aufrechterhaltung eines *Tools* oder für die Anpassung eines *Tools* verantwortlich ist/sind, ist/sind der/die Hersteller.

Anmerkung 2 zum Begriff: Die Bereitstellung von Skripts zur Automatisierung allgemeiner Funktionen modifiziert ein Tool oder passt es an.

3.14

Anforderung

Aussage, die ein Bedürfnis und dessen zugehörige Beschränkungen und Bedingungen vermittelt oder ausdrückt

Anmerkung 1 zum Begriff: Anforderungen sind auf verschiedenen Ebenen vorhanden und drücken die Bedürfnisse auf hohem Niveau aus (z. B. Anforderung an Softwarekomponenten).

[QUELLE: ISO/IEC IEEE 29148:2011, 4.1.17]

3.15

Analyse von Anforderungen

Prozess (3.12), durch den das Verständnis und die Priorisierung der *Anforderungen* (3.14) erreicht werden

3.16

Erfassen von Anforderungen

Prozess (3.12), durch den die *Anforderungen* (3.14) an einen Prozess ermittelt, überprüft, ausgedrückt und dokumentiert werden

3.17

Tool

in einem *Prozess* (3.12) eingesetzte Software, Hardware oder Firmware

3.18

Validierung

Bestätigung (3.4) durch Bereitstellung eines objektiven Nachweises, dass die *Anforderungen* (3.14) für einen spezifischen beabsichtigten Gebrauch oder eine spezifische beabsichtigte Anwendung erfüllt worden sind

Anmerkung 1 zum Begriff: Die Validierung eines *Prozesses* (3.12) wird durchgeführt, um sicherzustellen, dass er zweckdienlich ist, d. h. um sicherzustellen, dass der Prozess, soweit umgesetzt, auf beständige, wiederholbare und vergleichbare Weise zu den erwarteten Ergebnissen führt.

[QUELLE: ISO/IEC 27004:2009, 3.17, modifiziert — Anmerkung 1 zum Begriff wurde hinzugefügt.]

3.19

Validierungssatz

Reihe von objektiven Prüfungen mit eindeutig festgelegten Zielen, Eingaben und Ausgaben, die sich direkt auf die vereinbarten *Anforderungen* (3.14) des zu *validierenden* (3.18) *Prozesses* (3.12) beziehen

3.20

Verifizierung

Bestätigung (3.4) durch die Bereitstellung eines objektiven Nachweises, dass festgelegte Anforderungen erfüllt worden sind

Anmerkung 1 zum Begriff: Die Verifizierung versichert ausschließlich, dass ein Produkt seinen Spezifikationen entspricht.

[QUELLE: ISO/IEC 27004:2009, 3.18, modifiziert — die ursprüngliche Anmerkung wurde entfernt, Anmerkung 1 zum Begriff wurde hinzugefügt.]

3.21

Verifizierungsfunktion

Funktion, mit der verifiziert wird, ob zwei Datensätze identisch sind

[QUELLE: ISO/IEC 27037:2012, 3.25, modifiziert — die Anmerkungen wurden entfernt.]

3.22

White-Box-Test

Test, der die Inspektion von Details über die Verwirklichung umfasst

3.23

Arbeitsanweisung

ausführliche Beschreibung der Durchführungs- und Aufzeichnungsweise für einen *Prozess* (3.12)

4 Symbole und Abkürzungen

ATA AT Attachment

SATA Serial ATA

USB Universal Serial Bus

5 Entwicklung von Methoden und deren Sicherung

5.1 Überblick

Die Sicherung der Eignung und Angemessenheit von Vorfall-Ermittlungsmethoden kann erforderlich sein, um deutlich nachzuweisen, dass der Ermittler Methoden angewendet hat, die für die Ermittlung zweckdienlich sind, und dass er Methoden angewendet hat, die keine unannehmbaren Fehler oder Unsicherheiten aufweisen. Digitale Beweismittel, die aus der Anwendung von nicht gesicherten Methoden hervorgehen, können als grundsätzlich fehlerbehaftet und anfechtbar angesehen werden, was sie für die Zwecke der Ermittlungen wertlos machen kann.

Diese Norm liefert ein Sicherungsmodell, das alle Entwicklungsstufen der Tätigkeiten enthält, die in ihrer Gesamtheit eine Ermittlung bilden, wie in ISO/IEC 27042:2015 beschrieben, beginnend bei der einleitenden Spezifikation bis hin zum Einsatz und zur Aufrechterhaltung.

5.2 Allgemeine Grundsätze

Die Sicherung der Eignung und Angemessenheit von Vorfall-Ermittlungsmethoden sollte nach einem geeigneten Modell erfolgen, wie dem Planen-Durchführen-Prüfen-Handeln-Modell (Plan-Do-Check-Act) nach ISO/IEC 9001:2000, um sicherzustellen, dass alle Prozesse mindestens so oft einer Überprüfung unterzogen werden, wie sie auch angewendet werden.

5.3 Allgemeines Entwicklungs- und Einsatzmodell

Vor dem Einsatz eines Prozesses in Ermittlungen sollte er einen ordnungsgemäßen Entwicklungsprozess durchlaufen haben, um sicherzustellen, dass er zweckdienlich ist. Bild 2 zeigt folgende typische Stufen in diesem Prozess:

- Erfassung und Analyse von Anforderungen;
- Prozessgestaltung;
- Prozessverwirklichung;
- Prozessverifizierung (optional und unwesentlich);
- Prozessvalidierung;
- Bestätigung;
- Einsatz;
- Überprüfung und Aufrechterhaltung.

Jede dieser Stufen wird nachstehend ausführlicher erläutert.

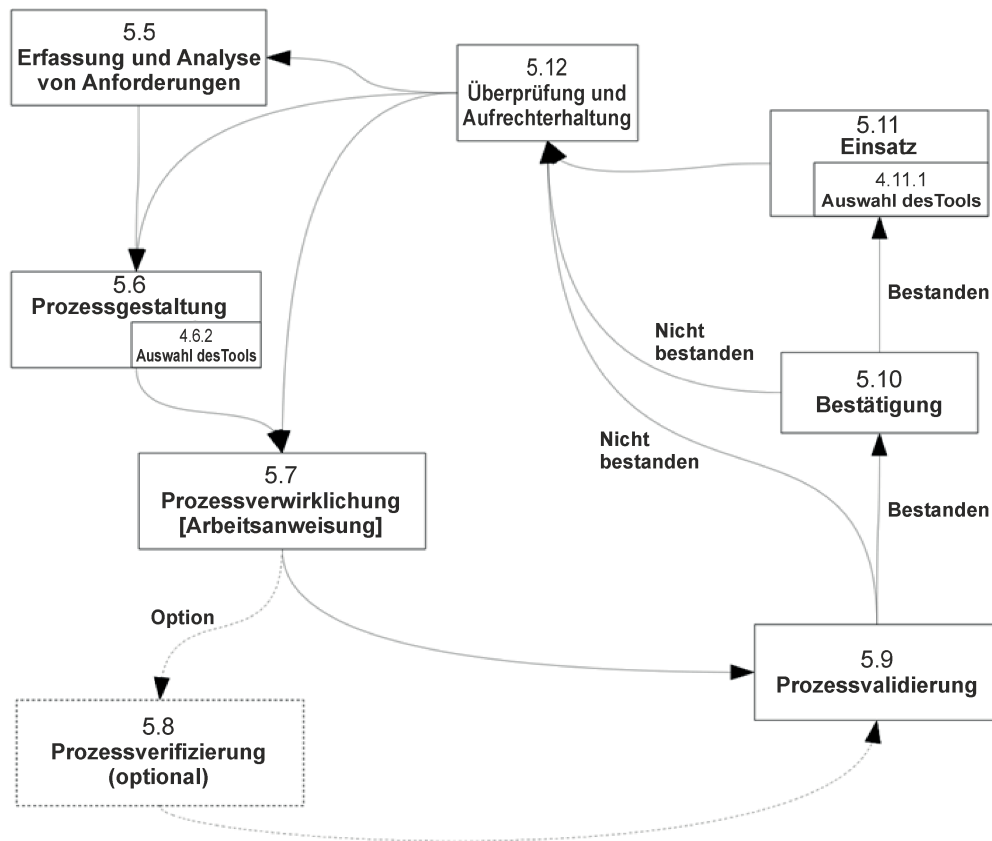


Bild 2 — Entwicklungs- und Einsatzprozess, einschließlich der Sicherungsstufen

5.4 Sicherungsstufen

Im vorstehenden Entwicklungsmodell sollte die Sicherung in den folgenden wesentlichen Sicherungsstufen erfolgen:

- Erfassung und Analyse von Anforderungen;
- Prozessvalidierung;
- Bestätigung;
- Überprüfung und Aufrechterhaltung.

ANMERKUNG Weitere Hinweise zur Durchführung dieser Stufen sind in der Beschreibung von Sicherungsmodellen in Abschnitt 5 enthalten.

5.5 Erfassung und Analyse von Anforderungen

5.5.1 Allgemeine Grundsätze der Anforderungen

Vor der Gestaltung eines Prozesses für den Einsatz in einer Untersuchung sollte eine angemessene Reihe von Anforderungen ausgearbeitet werden, die vom Auftraggeber akzeptiert und in Übereinstimmung mit bewährten Verfahrensweisen aufgezeichnet werden. Diese Reihe von Anforderungen sollte von den Anforderungen abgeleitet werden, die für die komplette Ermittlung festgelegt wurden, und darf sowohl funktionale als auch nicht funktionale Anforderungen umfassen.