

PRAXIS-LEITFADEN · STAND OKTOBER 2026

Tabletop Exercise: Der Praxis-Leitfaden

Tabletop-Übungen planen, moderieren und auditfest nachweisen – für ISMS-Manager und ISMS-Implementer

- Anforderungen aus ISO 27001, NIS2, DORA und BSI-Standard 200-4 auf einen Blick
- Übungsprogramm mit Beispiel-Jahresplan
- Vorbereitung in 7 Schritten, Moderationsleitfaden für 60 und 90 Minuten
- Einsatzbereites Ransomware-Szenario mit Injects und Leitfragen
- Beobachtungsbogen, Maßnahmenplan, Nachweis-Dokumente und Checkliste zum Ausdrucken

Über diesen Leitfaden

Eine Tabletop-Übung ist der schnellste Weg, um herauszufinden, ob Ihre Pläne für den Ernstfall tragen – und der günstigste Weg, das gegenüber Auditoren und Aufsicht zu belegen. Dieser Leitfaden führt Sie von der Planung über die Moderation bis zum Nachweis.

1	Was ist eine Tabletop Exercise?	Grundlagen
2	Warum üben? Anforderungen im Überblick	ISO 27001 · NIS2 · DORA · BSI
3	Das Übungsprogramm: wie oft, was, wer	ISMS-Manager
4	Vorbereitung in 7 Schritten	ISMS-Implementer
5	Moderationsleitfaden für 60 und 90 Minuten	ISMS-Implementer
6	Beispielszenario: Ransomware im Produktionsnetz	einsatzbereit
7	Beobachtungsbogen	Kopiervorlage
8	Auswertung: Hotwash, After-Action-Report, Maßnahmenplan	beide
9	Der auditfeste Nachweis	ISMS-Manager
10	Checkliste: Tabletop-Übung in drei Phasen	Kopiervorlage
11	Quellen, Vorlagen und weiterführende Informationen	Anhang

Für ISMS-Manager

„Welche Übungen brauchen wir, wann machen wir sie und wie entstehen daraus Verbesserungen?“

Lesen Sie vor allem Kapitel 2, 3, 8 und 9:
Anforderungen, Übungsprogramm,
Maßnahmenverfolgung und
Nachweisführung.

Für ISMS-Implementer

„Wie baue und moderiere ich die konkrete Übung, damit sie realistisch und nützlich ist?“

Lesen Sie vor allem Kapitel 4 bis 7 und 10:
Vorbereitung, Moderation, Szenario,
Beobachtungsbogen und Checkliste.

Hinweis

Dieser Leitfaden dient der allgemeinen Information und ersetzt keine Rechtsberatung. Maßgeblich sind die jeweils geltenden Gesetzes-, Verordnungs- und Normtexte. Normanforderungen aus ISO/IEC 27001 und ISO 22301 sind sinngemäß wiedergegeben.

Was ist eine Tabletop Exercise?

Eine **Tabletop Exercise** – auf Deutsch **Tabletop-Übung**, oft auch Table-Top-Übung geschrieben – ist eine moderierte, diskussionsbasierte Übung, in der ein Team einen realistischen Vorfall Schritt für Schritt durchspielt, ohne dass Systeme abgeschaltet oder Maßnahmen real ausgeführt werden. Eine Moderatorin oder ein Moderator spielt zu festgelegten Zeitpunkten neue Lageinformationen ein, sogenannte **Injects**. Die Teilnehmenden entscheiden in ihren echten Rollen: Wer bewertet den Vorfall? Wer eskaliert, wer informiert die Geschäftsleitung, wer meldet an die Behörde, was sagen wir Kunden?

Geprüft werden nicht die Menschen, sondern die Pläne und Abläufe: Sind Rollen klar, funktionieren Alarmierung und Eskalation, liegen die nötigen Informationen vor, und kennt jeder seine Befugnisse? Die US-Behörde NIST beschreibt Tabletop Exercises in der SP 800-84 als diskussionsbasierte Übung, in der Beteiligte ihre Rollen und Reaktionen in einem Szenario besprechen. In der Praxis haben sich kompakte Formate von 60 bis 90 Minuten bewährt, weil sie regelmäßig wiederholbar sind.

Tabletop oder Table Top?

Beide Schreibweisen sind gebräuchlich. Im Englischen hat sich „tabletop exercise“ durchgesetzt, im Deutschen finden Sie „Tabletop-Übung“ und „Table-Top-Übung“. Gemeint ist dasselbe: eine Übung „am Tisch“.

Tabletop-Übung im Vergleich mit anderen Übungsformen

Übungsform	Was passiert	Aufwand	Wofür geeignet
Planbesprechung walkthrough	Ein Notfallplan wird mit den vorgesehenen Rollen durchgesprochen und auf Plausibilität, Vollständigkeit und Aktualität geprüft.	niedrig	Neue oder geänderte Pläne
Tabletop-Übung tabletop exercise	Ein Szenario mit Injects wird moderiert durchgespielt; Entscheidungen und Kommunikation stehen im Mittelpunkt.	niedrig bis mittel	Rollen, Eskalation, Entscheidungen, Meldewege
Stabsübung	Der Krisen- oder Notfallstab arbeitet ein Szenario mit Lagebesprechungen, Protokoll und Visualisierung ab.	mittel	Zusammenarbeit im Stab, Führungszyklus
Funktionstest functional exercise / test	Eine Maßnahme wird real ausgeführt, etwa ein Restore- oder Umschalttest.	mittel bis hoch	Technische Wiederanlauffähigkeit
Stabsrahmen- oder Vollübung full-scale exercise	Stab und operative Teams üben gemeinsam, bis hin zu allen Hierarchieebenen.	hoch	Organisationsweite Zusammenarbeit
Red Teaming / TLPT	Ein realer, kontrollierter Angriff prüft Erkennung und Abwehr.	sehr hoch	Technische Abwehr, Detektion

Begriffe nach BSI-Standard 200-4, Kapitel 13 „Üben und Testen“, ergänzt um international gebräuchliche Bezeichnungen.

Warum üben? Anforderungen im Überblick

Kein Regelwerk schreibt wörtlich „Tabletop-Übung“ vor. Aber alle relevanten Regelwerke verlangen, dass Incident- und Notfallprozesse wirksam sind – und genau das belegt eine dokumentierte Übung.

Regelwerk	Fundstelle	Was verlangt wird (sinngemäß)	Was eine Übung belegt
ISO/IEC 27001:2022	Anhang A, A.5.24–A.5.28	Incident-Management planen und vorbereiten, Ereignisse beurteilen, auf Vorfälle reagieren, aus Vorfällen lernen, Beweismaterial sichern	Rollen, Eskalation und Entscheidungen funktionieren; Erkenntnisse fließen in Maßnahmen
ISO/IEC 27001:2022	A.5.29, A.5.30	Informationssicherheit bei Störungen; IKT-Bereitschaft für Business Continuity planen, umsetzen, aufrechterhalten und testen	Wiederanlaufannahmen und Abhängigkeiten sind plausibel
ISO/IEC 27001:2022	9.1, 9.2, 9.3, 10.2	Wirksamkeit überwachen und messen, intern auditieren, in der Managementbewertung berücksichtigen, Korrekturmaßnahmen umsetzen	Report, Kennzahlen und Maßnahmenplan als Eingaben
NIS2 – RL (EU) 2022/2555	Art. 21 Abs. 2 lit. b, c, f	„Bewältigung von Sicherheitsvorfällen“; „Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement“; Konzepte und Verfahren zur Bewertung der Wirksamkeit der Risikomanagementmaßnahmen	Wirksamkeit der Maßnahmen ist bewertet und dokumentiert
Umsetzung Deutschland	§ 30 Abs. 2 Nr. 2, 3, 6 BSIG; § 38 Abs. 3 BSIG	Mindestmaßnahmen analog Art. 21; Geschäftsleitungen müssen regelmäßig an Schulungen teilnehmen	Geschäftsleitung ist eingebunden und geschult
Umsetzung Österreich	§ 32 Abs. 4 lit. b, c, f NISG 2026; § 31 Abs. 2 NISG 2026	Mindestmaßnahmen analog Art. 21; Leitungsorgane müssen an Cybersicherheitsschulungen teilnehmen	wie oben
NIS2	Art. 23 Abs. 4	Erhebliche Sicherheitsvorfälle melden: Frühwarnung binnen 24 Stunden, Meldung binnen 72 Stunden, Abschlussbericht binnen eines Monats	Meldekette und Fristen sind geübt

Regelwerk	Fundstelle	Was verlangt wird (sinngemäß)	Was eine Übung belegt
DORA – VO (EU) 2022/2554	Art. 11 Abs. 6	Finanzunternehmen testen IKT-Geschäftsfortführungspläne sowie IKT-Reaktions- und Wiederherstellungspläne mindestens jährlich und bei wesentlichen Änderungen; Krisenkommunikationspläne werden getestet	Jährlicher Testnachweis
BSI-Standard 200-4	Kapitel 13	Stabsübung und Alarmierungsübung regelmäßig durchführen (Pflicht bereits im Reaktiv-BCMS); Jahresübungsplanung, die mindestens zwölf Monate umfassen sollte; Übungskonzept für jede Übung	Systematisches Übungsprogramm
ISO 22301:2019	Abschnitt 8.5	Ein Übungsprogramm, mit dem Business-Continuity-Strategien und -Pläne regelmäßig geprüft werden	Planmäßiges, dokumentiertes Üben

Merke

Für den Nachweis zählt nicht, dass geübt wurde, sondern was dabei herauskam: dokumentierte Entscheidungen, Findings und umgesetzte Maßnahmen. Kapitel 9 zeigt, welche Dokumente Sie dafür brauchen.

KAPITEL 3

Das Übungsprogramm: wie oft, was, wer

Eine einzelne Übung ist ein Schnappschuss. Wirksam wird Üben erst als Programm: geplant, risikobasiert und mit nachverfolgten Ergebnissen.

Wie oft sollte man üben?

ISO/IEC 27001 nennt keine feste Frequenz; die Häufigkeit leitet sich aus Ihrer Risikobewertung ab. Konkrete Orientierung geben andere Regelwerke:

- **BSI-Standard 200-4** nennt als Beispiel: Stabsübung mindestens jährlich mit allen Stabsmitgliedern einschließlich der Stellvertretungen; Planbesprechung zeitnah nach Erstellung oder wesentlicher Änderung eines Plans; Funktionstest mindestens jährlich für Prozesse und Ressourcen mit einer Wiederanlaufzeit (RTO) unter 24 Stunden, mindestens alle drei Jahre bei einem RTO unter fünf Tagen.
- **DORA** verlangt von Finanzunternehmen mindestens jährliche Tests der IKT-Geschäftsfortführungs- sowie Reaktions- und Wiederherstellungspläne.
- **Praxis:** mindestens eine Tabletop-Übung pro Jahr für jedes kritische Szenario, zusätzlich anlassbezogen – nach einem realen Vorfall, nach größeren Änderungen an Organisation, Systemen oder Dienstleistern und wenn neue Personen Schlüsselrollen übernehmen.

Beispiel: Jahresübungsplan für ein mittelständisches Unternehmen

BEISPIEL – AN IHRE RISIKOBEWERTUNG ANPASSEN

Quartal	Übungsform	Szenario	Teilnehmende	Belegt u. a.
Q1	Tabletop-Übung	Ransomware-Angriff auf zentrale Systeme	IT-Betrieb, IR-/SOC-Team, Informationssicherheit	ISO 27001 A.5.24–A.5.26 · NIS2 Art. 21 Abs. 2 lit. b
Q2	Stabsübung	Eskalierter Cybervorfall mit Meldepflicht und Außenkommunikation	Krisenstab mit Geschäftsleitung, Kommunikation, Recht/Datenschutz	ISO 27001 A.5.24, A.5.29 · NIS2 Art. 21 Abs. 2 lit. c
Q3	Tabletop-Übung	Ausfall oder Kompromittierung eines kritischen Dienstleisters	Informationssicherheit, IT, Lieferantenmanagement, Fachbereiche	ISO 27001 A.5.24–A.5.27 · NIS2 Art. 21 Abs. 2 lit. d
Q4	Planbesprechung + Funktionstest	Wiederanlauf der kritischen IT nach einem Totalausfall	IT-Betrieb, BCM, System- und Prozessverantwortliche	ISO 27001 A.5.30 · NIS2 Art. 21 Abs. 2 lit. c

Wer nimmt teil?

Rolle	Aufgabe in der Übung
Moderation	Führt durch Agenda und Injects, hält die Zeit, löst nichts selbst.
Protokoll und Beobachtung	Hält Entscheidungen mit Uhrzeit fest und bewertet anhand vorab festgelegter Kriterien.
IT-Betrieb und Incident Response	Bewertet die technische Lage, schlägt Eindämmung und Wiederanlauf vor.
Informationssicherheit (ISB/CISO)	Stuft Ereignisse ein, verantwortet den Incident-Prozess.
Geschäftsleitung bzw. Krisenstab	Trifft Entscheidungen mit Geschäftsrelevanz, gibt Kommunikation frei.
Kommunikation	Steuert interne und externe Kommunikation.
Recht und Datenschutz	Prüft Meldepflichten und rechtliche Folgen.
Betroffene Fachbereiche, ggf. Dienstleister	Bewerten Auswirkungen auf Kernprozesse und Lieferketten.

Entscheidend ist, dass echte Entscheiderinnen und Entscheider am Tisch sitzen. Beziehen Sie regelmäßig auch die Stellvertretungen ein – im Ernstfall ist nicht jede Person erreichbar.

KAPITEL 4

Vorbereitung in 7 Schritten

Eine gute Tabletop-Übung entsteht in der Vorbereitung: Je klarer Ziele, Szenario und Rollen sind, desto mehr lernt das Team in der Übung. Vorlagen nehmen Ihnen den größten Teil der Arbeit ab.

1. Übungsziele festlegen

Formulieren Sie zwei bis vier überprüfbare Ziele und verknüpfen Sie sie mit einem Risiko oder Control. Beispiele: „Das Team stuft einen Ransomware-Befall nach den Kriterien des IR-Plans ein und alarmiert den Krisenstab.“ – „Die Meldeverantwortung für die 24-Stunden-Frühwarnung ist geklärt.“ – „Die Wiederanlaufreihenfolge der kritischen Systeme ist abgestimmt.“

2. Scope und Format bestimmen

Welche Pläne werden geprüft (IR-Plan, Notfallhandbuch, Krisenkommunikationsplan)? Wer nimmt teil? 60 oder 90 Minuten, vor Ort oder remote? Was ist ausdrücklich nicht Teil der Übung?

3. Szenario wählen

Leiten Sie das Szenario aus Ihrem Risikoregister und der Business Impact Analyse ab: Was würde Ihre kritischsten Prozesse am stärksten treffen? Das Szenario muss realistisch sein, aber nicht technisch perfekt. Fassen Sie es in zwei Sätzen zusammen, bevor Sie Details ausarbeiten.

4. Injects schreiben und in der MSEL festhalten

Ein Inject ist eine Lageinformation, die zu einem festgelegten Zeitpunkt eingespielt wird – als Anruf, Ticket, E-Mail oder Presseanfrage. Jeder Inject zielt auf ein Übungsziel und erzwingt eine Entscheidung. Halten Sie Zeitpunkt, Absender, Inhalt und erwartete Reaktion in einer **MSEL** (Master Scenario Events List) fest und planen Sie Reserve-Injects ein.

Zeit	Absender / Kanal	Inject	Erwartete Reaktion / Übungsziel
T+0	Service Desk, Ticket	Mehrere Nutzende melden, dass Dateien nicht mehr geöffnet werden können.	Ereignis bewerten, IR-Team einbinden (Ziel 1)
T+15	IT-Betrieb, Anruf	Auf zwei Servern liegen Erpresserschriften; Backups werden geprüft.	Als Vorfall einstufen, Krisenstab alarmieren
T+35	Angreifer, E-Mail	Drohung, exfiltrierte Daten in 24 Stunden zu veröffentlichen.	Meldepflichten prüfen, Meldeverantwortung festlegen (Ziel 2)

AUSZUG – DAS VOLLSTÄNDIGE SZENARIO FOLGT IN KAPITEL 6

5. Rollen besetzen

Benennen Sie Moderation, Protokoll und mindestens eine beobachtende Person. Die Spielenden übernehmen ihre realen Rollen; wer fehlt, wird nicht „mitgespielt“, sondern als Lücke notiert.

6. Unterlagen bereitstellen

Legen Sie die Pläne bereit, die im Ernstfall verfügbar wären – in der Form, in der sie verfügbar wären. Liegt das Notfallhandbuch nur im Cloud-Speicher, der im Szenario ausfällt, ist genau das ein Finding.

7. Übungskonzept dokumentieren

Der BSI-Standard 200-4 verlangt für jede Übung ein Übungskonzept. Es muss nicht lang sein, sollte aber enthalten: Anlass und Bezug (Risiko, Control, Jahresplan), Übungsziele, Szenario und Scope, Teilnehmende und Rollen, Ablauf und Agenda, Bewertungskriterien, Dokumentation und Termin. Das Übungskonzept ist zugleich das erste Dokument Ihres Nachweises (Kapitel 9).

Moderationsleitfaden für 60 und 90 Minuten

Ein Moderationsleitfaden – im Englischen *facilitator guide* – legt fest, was die Moderation in welcher Phase tut. Diese Agenda funktioniert für die meisten Szenarien.

Phase	90 Min.	60 Min.	Inhalt
Einweisung	0–10	0–5	Ziele, Spielregeln, Rollen. Geprüft werden Pläne, nicht Personen.
Ausgangslage	10–20	5–10	Szenario vorlesen, erste Lagebewertung, Führung klären.
Phase 1: Erkennung & Bewertung	20–40	10–25	Vorfall einstufen, alarmieren, eskalieren.
Phase 2: Eskalation & Eindämmung	40–65	25–40	Eindämmung entscheiden, Meldepflichten prüfen, externe Anfragen beantworten.
Phase 3: Kommunikation & Wiederanlauf	65–75	40–50	Stakeholder informieren, Wiederanlauf priorisieren.
Hotwash	75–90	50–60	Was lief gut, was fehlte? Erste Maßnahmen mit Verantwortlichen.

Spielregeln für die Einweisung

- Wir prüfen Pläne und Abläufe, nicht die Leistung einzelner Personen.
- Handeln Sie so, wie Sie es im Ernstfall tun würden – mit den Informationen, die Ihnen vorliegen.
- Nehmen Sie die Lage als gegeben. Diskussionen über die Wahrscheinlichkeit des Szenarios kommen in den Hotwash.
- Was im Raum gesagt wird, dient der Verbesserung und wird nicht personenbezogen bewertet.

Moderationsfragen für jede Phase

- **Erkennung & Bewertung:** Woran würden wir das real bemerken? Ist das ein Sicherheitsvorfall – und wer entscheidet das? Wen alarmieren wir?
- **Eskalation & Eindämmung:** Welche Entscheidung muss jetzt fallen, und wer ist befugt? Was nehmen wir in Kauf? Welche Fristen laufen – etwa 24 Stunden für die NIS2-Frühwarnung oder 72 Stunden für die Meldung einer Datenschutzverletzung?
- **Kommunikation:** Was sagen wir Beschäftigten, Kunden, Dienstleistern und Presse – und wer gibt frei?
- **Wiederanlauf:** In welcher Reihenfolge fahren wir Prozesse wieder hoch? Woran erkennen wir, dass der Angreifer nicht mehr im Netz ist?
- **Hotwash:** Was hat funktioniert? Wo fehlten Informationen oder Befugnisse? Was im Plan ist veraltet?

Tipps für die Moderation

- **Zeit halten:** Spielen Sie Injects pünktlich ein, auch wenn eine Diskussion noch läuft – im Ernstfall wartet die Lage auch nicht.
- **Nicht lösen:** Geben Sie keine Antworten vor. Fragen Sie nach: „Wo steht das im Plan?“

- **Entscheidungen festhalten:** Lassen Sie jede Entscheidung mit Uhrzeit und entscheidender Person protokollieren.
- **Parkplatz nutzen:** Wichtige Nebenthemen notieren und im Hotwash aufgreifen.
- **Alle einbeziehen:** Sprechen Sie stille Rollen gezielt an, etwa Recht oder Kommunikation.

KAPITEL 6

Beispielszenario: Ransomware im Produktionsnetz

Ein einsatzbereites Szenario für eine 90-minütige Tabletop-Übung. Passen Sie Systeme, Rollen und Uhrzeiten an Ihre Organisation an. Sieben weitere Szenarien mit Injects und Leitfragen finden Sie unter secdrills.com/wissen/tabletop-szenarien/.

Ausgangslage (vorlesen)

Donnerstag, 16:40 Uhr. Der Service Desk erhält in kurzer Folge Meldungen aus Vertrieb und Buchhaltung: Dateien auf dem zentralen Fileserver lassen sich nicht mehr öffnen und tragen eine unbekannte Dateierdung. Kurz darauf meldet die Fertigungsleitung, dass die Auftragsdaten im ERP-System nicht mehr abrufbar sind. Die IT-Leitung ist auf dem Heimweg, die stellvertretende Leitung im Urlaub.

Übungsziele

1. Der Vorfall wird nach den Kriterien des Incident-Response-Plans eingestuft und der Krisenstab innerhalb der vorgesehenen Zeit alarmiert.
2. Die Entscheidung über Isolierung und Produktionsstopp wird von der befugten Person getroffen und dokumentiert.
3. Meldepflichten werden erkannt, und die Meldeverantwortung ist geklärt.

Injects

Zeit	Inject	Leitfragen für die Moderation
T+0	Service Desk meldet nicht lesbare Dateien auf dem Fileserver und Ausfall des ERP-Zugriffs.	Wer bewertet das Ereignis? Nach welchen Kriterien? Wer wird jetzt informiert?
T+15	Auf mehreren Servern liegt ein Erpresserschreiben. Die Prüfung der Backups läuft.	Ist das ein Sicherheitsvorfall? Wird der Krisenstab alarmiert – von wem, über welchen Kanal?
T+25	Die Fertigungsleitung fragt, ob die Produktion weiterlaufen kann. Die Linien sind noch in Betrieb.	Isolieren oder weiterlaufen lassen? Wer darf den Produktionsstopp freigeben?
T+35	E-Mail der Angreifer: Exfiltrierte Kundendaten werden in 24 Stunden veröffentlicht, wenn nicht gezahlt wird.	Welche Meldepflichten entstehen (NIS2, Datenschutz)? Wer meldet bis wann? Nach welchen Kriterien wird über eine Zahlung entschieden?
T+50	Ein Großkunde ruft an: Er hat Gerüchte über einen Angriff gehört und fragt nach Lieferfähigkeit.	Wer spricht mit dem Kunden? Was darf gesagt werden? Wer gibt frei?

Zeit	Inject	Leitfragen für die Moderation
T+65	Die IT meldet: Die letzten Offline-Backups sind vier Tage alt; ein Wiederanlauf des ERP dauert voraussichtlich drei Tage.	Welche Prozesse haben Vorrang? Welche Notbetriebsverfahren greifen? Was bedeutet das für Kunden und Lieferanten?

Hinweise für die Moderation

- Wenn niemand die Isolierung entscheidet: Fragen Sie nach der Befugnis im Plan, nicht nach der richtigen Antwort.
- Wenn die Meldefristen nicht angesprochen werden: Spielen Sie T+35 unverändert ein und fragen Sie nach der Frist.
- Reserve-Inject, falls das Team schnell ist: Eine Journalistin fragt nach einer Stellungnahme bis 19 Uhr.

Beobachtungsbogen

Beobachtende greifen nicht ein, sondern notieren mit Uhrzeit, was geschieht. Legen Sie die Kriterien vorab aus den Übungszielen fest. Die Beobachtungen sind die Rohdaten für den After-Action-Report.

Übung: _____ Datum: _____ Beobachter/in: _____

Kriterium	Leitfrage	Uhrzeit	Beobachtung	Bewertung erfüllt / teilw. / nicht
Lageerfassung & Einstufung	Rechtzeitig erkannt und nach Kriterien eingestuft?			☐ ☐ ☐
Alarmierung & Eskalation	Richtige Personen über vorgesehene Wege erreicht?			☐ ☐ ☐
Entscheidungen	Wer hat was entschieden, mit welcher Befugnis?			☐ ☐ ☐
Meldepflichten	Fristen erkannt, Meldeverantwortung geklärt?			☐ ☐ ☐
Kommunikation	Intern und extern abgestimmt, Freigabe geklärt?			☐ ☐ ☐
Nutzung der Pläne	Wurde der Plan genutzt – und hat er getragen?			☐ ☐ ☐
Wiederanlauf	Prioritäten abgestimmt und mit RTO/RPO abgeglichen?			☐ ☐ ☐
Weitere Beobachtungen	Lücken, fehlende Informationen, Überraschungen			

Beispiele für gute Beobachtungen

- „Einstufung als Sicherheitsvorfall erst 25 Minuten nach dem ersten Inject; die Kriterien im IR-Plan waren nicht bekannt.“
- „Die Stellvertretung der IT-Leitung fehlt in der Alarmierungsliste.“
- „Isolierung vertagt, weil unklar war, wer einen Produktionsstopp freigeben darf.“
- „24-Stunden-Frist erkannt, aber niemand als meldeverantwortlich benannt.“

Gute Beobachtungen sind konkret, datiert und beschreiben einen Sachverhalt, keine Person.

Auswertung: Hotwash, After-Action-Report, Maßnahmenplan

Der Wert einer Übung entsteht nach der Übung. Ohne Auswertung und Maßnahmenverfolgung bleibt sie ein Gesprächstermin.

Hotwash: direkt im Anschluss

Nehmen Sie sich 10 bis 15 Minuten unmittelbar nach dem letzten Inject, solange die Eindrücke frisch sind. Vier Fragen genügen: Was war geplant? Was ist tatsächlich passiert? Warum gab es Abweichungen? Was ändern wir?

After-Action-Report: innerhalb weniger Tage

Der After-Action-Report (AAR) fasst die Übung prüffähig zusammen. Bewährte Gliederung:

1. Übungsüberblick: Datum, Szenario, Ziele, Teilnehmende und Rollen
2. Ablauf: Injects und zentrale Entscheidungen mit Zeitstempeln
3. Bewertung je Übungsziel: erreicht, teilweise erreicht, nicht erreicht – mit Begründung
4. Stärken: was beibehalten werden soll
5. Findings: Lücken in Plänen, Rollen, Informationen oder Befugnissen
6. Maßnahmenplan (siehe unten) und Termin der Folgeübung

Maßnahmenplan: vom Finding zur wirksamen Maßnahme

Finding	Maßnahme	Owner	Frist	Prio	Status	Wirksamkeitsprüfung
BEISPIEL Stellvertretung der IT-Leitung fehlt in der Alarmierungsliste	Alarmierungsliste ergänzen, Erreichbarkeit testen	ISB	2 Wochen	hoch	offen	Alarmierungsübung im nächsten Quartal
BEISPIEL Befugnis für Produktionsstopp ungeklärt	Entscheidungsbefugnis im IR-Plan festlegen, Geschäftsleitung freigeben lassen	CISO	4 Wochen	hoch	offen	Folgeübung mit gleichem Inject

Lessons Learned richtig formulieren

So nicht

- „Die Kommunikation war schlecht.“
- „Wir müssen schneller werden.“
- „Herr M. hat zu spät reagiert.“

So besser

- „Für Kundenanfragen gab es keine freigegebene Sprachregelung.“
- „Die Einstufung dauerte 25 Minuten, weil die Kriterien im Plan fehlen.“
- „Die Alarmierungsliste enthält keine Stellvertretung.“

Eine Maßnahme gilt erst als wirksam, wenn eine Folgeübung zeigt, dass das Problem nicht mehr auftritt. Diese Prüfung schließt den Kreis zu ISO 27001 A.5.27 (Erkenntnisse aus Vorfällen) und Abschnitt 10.2 (Korrekturmaßnahmen).

KAPITEL 9

Der auditfeste Nachweis

Auditoren und Aufsicht wollen nicht hören, dass geübt wurde – sie wollen es sehen. Diese acht Dokumente bilden einen vollständigen Übungsnachweis.

#	Dokument	Inhalt	Liegt vor
1	Übungsauftrag & Ziele	Anlass, Bezug zu Risiko, Control und Jahresplan, Übungsziele	☐
2	Szenario & Scope	Szenario, geprüfte Pläne, Abgrenzung	☐
3	Teilnehmende & Rollen	Namen, Funktionen, Rollen in der Übung, Stellvertretungen	☐
4	Ablaufprotokoll	Injects, Entscheidungen und Begründungen mit Zeitstempeln	☐
5	Beobachtungen / Findings	Ausgefüllte Beobachtungsbögen, festgestellte Lücken	☐
6	After-Action-Report	Bewertung je Übungsziel, Stärken, Findings	☐
7	Maßnahmenplan	Maßnahmen mit Owner, Frist, Priorität und Status	☐
8	Nachweis der Umsetzung & Wirksamkeit	Erledigte Maßnahmen, Ergebnis der Folgeübung	☐

Kennzahlen für das Übungsprogramm

BEISPIELE – KEINE NORMVORGABEN

Kennzahl	Was sie zeigt	Datenquelle
Anteil der kritischen Szenarien, die pro Jahr geübt wurden	Abdeckung des Übungsprogramms gegenüber der Risikobewertung	Jahresübungsplan, Risikoregister

Kennzahl	Was sie zeigt	Datenquelle
Zeit bis zur Eskalation	Wie schnell ein Ereignis bewertet und eskaliert wird (A.5.25)	Ablaufprotokoll
Abschlussquote der Maßnahmen innerhalb der Frist	Ob Erkenntnisse tatsächlich umgesetzt werden (A.5.27, 10.2)	Maßnahmenplan
Wiederholte Findings	Ob Korrekturmaßnahmen wirken	Vergleich über mehrere Übungen
Teilnahmequote der vorgesehenen Rollen inkl. Stellvertretungen	Ob Rollen im Ernstfall besetzt wären	Teilnehmerliste

Nutzen Sie Report und Kennzahlen als Eingaben für das interne Audit (ISO 27001, 9.2) und die Managementbewertung (9.3). Über mehrere Übungen hinweg zeigen sie den Reifegrad-Trend Ihrer Notfall- und Incident-Prozesse.

Checkliste: Tabletop-Übung in drei Phasen

Vorbereitung

- ☐ Übung ist im Jahresübungsplan verankert
- ☐ 2–4 überprüfbare Übungsziele mit Bezug zu Risiko oder Control
- ☐ Szenario aus Risikoregister bzw. BIA abgeleitet
- ☐ Injects und Reserve-Injects in der MSEL
- ☐ Moderation, Protokoll und Beobachtung benannt
- ☐ Entscheiderinnen und Entscheider eingeladen, Termin bestätigt
- ☐ Pläne und Kontaktlisten in realistischer Form bereitgelegt
- ☐ Beobachtungsbogen mit Kriterien vorbereitet
- ☐ Übungskonzept dokumentiert und freigegeben

Durchführung

- ☐ Einweisung mit Zielen und Spielregeln
- ☐ Injects pünktlich eingespielt
- ☐ Entscheidungen mit Uhrzeit und Person protokolliert
- ☐ Meldepflichten und Fristen angesprochen
- ☐ Stille Rollen gezielt einbezogen
- ☐ Hotwash direkt im Anschluss durchgeführt

Nachbereitung

- ☐ After-Action-Report innerhalb weniger Tage erstellt
- ☐ Bewertung je Übungsziel dokumentiert
- ☐ Findings in Maßnahmen mit Owner, Frist und Priorität überführt
- ☐ Maßnahmenplan an Verantwortliche verteilt
- ☐ Status der Maßnahmen regelmäßig verfolgt
- ☐ Pläne aktualisiert (IR-Plan, Notfallhandbuch, Kontaktlisten)
- ☐ Folgeübung zur Wirksamkeitsprüfung terminiert
- ☐ Alle acht Nachweis-Dokumente abgelegt
- ☐ Ergebnisse in internes Audit und Managementbewertung eingebracht

Tipp

Halten Sie die erste Übung klein: ein Szenario, ein Team, 60 Minuten. Wer regelmäßig in kurzen Formaten übt, lernt mehr als mit einer großen Übung alle paar Jahre.

Quellen, Vorlagen und weiterführende Informationen

Primärquellen

- BSI-Standard 200-4 Business Continuity Management, Kapitel 13 „Üben und Testen“ – bsi.bund.de
- ISO/IEC 27001:2022 Informationssicherheitsmanagementsysteme – iso.org/standard/27001
- ISO 22301:2019 Business Continuity Management Systems – iso.org
- Richtlinie (EU) 2022/2555 (NIS2), Art. 21 und Art. 23 – eur-lex.europa.eu, CELEX:32022L2555
- Verordnung (EU) 2022/2554 (DORA), Art. 11 – eur-lex.europa.eu, CELEX:32022R2554
- BSI-Gesetz in der Fassung des NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes, §§ 30, 32, 38 – BGBl. 2025 I Nr. 301
- Netz- und Informationssystemsicherheitsgesetz 2026 (NISG 2026), §§ 31, 32, 34 – BGBl. I Nr. 94/2025
- NIST SP 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities – csrc.nist.gov/pubs/sp/800/84/final
- NIST SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management – csrc.nist.gov/pubs/sp/800/61/r3/final
- CISA Tabletop Exercise Packages (CTEP) – cisa.gov
- NCSC Exercise in a Box – ncsc.gov.uk

Kostenlose Vorlagen von SecDrills

- [Tabletop-Szenario-Vorlage](https://secdrills.com/vorlagen/tabletop-szenario-vorlage.html) – secdrills.com/vorlagen/tabletop-szenario-vorlage.html
- [After-Action-Review-Vorlage](https://secdrills.com/vorlagen/after-action-review-vorlage.html) – secdrills.com/vorlagen/after-action-review-vorlage.html
- [Incident-Response-Plan-Vorlage](https://secdrills.com/vorlagen/incident-response-plan-vorlage.html) – secdrills.com/vorlagen/incident-response-plan-vorlage.html
- [IT-Notfallplan-Vorlage](https://secdrills.com/vorlagen/it-notfallplan-vorlage.html) – secdrills.com/vorlagen/it-notfallplan-vorlage.html

Weiterlesen auf secdrills.com

- [Tabletop Exercise: Definition, Ablauf und Beispiele](#)
- [Tabletop-Szenarien: 8 Beispiele mit Injects und Leitfragen](#)
- [Notfallübung: Übungsarten, Häufigkeit und Checkliste](#)
- [ISO 27001 Notfallmanagement: Anhang A 5.24–5.30 üben und nachweisen](#)
- [After-Action-Review: Ablauf, Vorlage und Maßnahmenplan](#)
- [MSEL: das Drehbuch jeder Übung](#)

Tabletop-Übungen ohne Organisationsaufwand

Dieser Leitfaden zeigt, was eine gute Tabletop-Übung ausmacht. SecDrills nimmt Ihnen die Arbeit dahinter ab.

- **Geführte Übungen im Browser:** vordefinierte Szenarien mit Injects, ohne Installation und ohne externen Moderator.
- **Erste Übung ab 30 Minuten:** kompakte Formate, die sich regelmäßig wiederholen lassen.
- **Rollen nach ECSF, Methodik orientiert an ENISA:** Jede Person übt in ihrer realen Funktion.
- **Automatischer, auditierbarer After-Action-Report:** Entscheidungen, Zeitstempel und Findings als Nachweis für ISO 27001, NIS2 und TISAX.

Wie übungsbereit ist Ihre Organisation?

Der kostenlose Übungsreife-Check zeigt in wenigen Minuten, wo Sie stehen: secdrills.com/check/

Herausgeber: BlueGravitas GmbH, 8570 Voitsberg, Österreich, FN 678630 k · secdrills.com · Stand: Oktober 2026

Dieser Leitfaden darf mit Quellenangabe frei weitergegeben werden. Er dient der allgemeinen Information und ersetzt keine Rechts- oder Normberatung.