Heft 43 | Juli 2026 | 20. Jahrgang | ISSN 1864-6557

IT-GOVERNANCE

Fachzeitschrift des ISACA Germany Chapter e. V.

- → Grenzen der IT-Risikomodellierung
- → Implementierung von Informationssicherheit
- → Tech-orientierte Due Diligence
- → BYOD – Bring Your Own Device
- → Wissensmanagement in der Wirtschaftsprüfung

ISACA Germany Chapter e.V.

dpunkt.verlag | it-governance.dpunkt.de | isaca.de

BYOD messbar machen: ein Praxisansatz mit COBIT 19 und IT-BSC

Markus Groß

Bring Your Own Device (BYOD) erzeugt Zielkonflikte zwischen Nutzererlebnis, Sicherheit und Nachweisführung. Der Beitrag zeigt, wie BYOD mithilfe der Balanced Scorecard (BSC), COBIT 19 und einem klar definierten Informationsmodell steuerbar wird. Regulatorische Leitplanken – DORA, NIS-2, EU AI Act und ISO/IEC 27001 – werden in ein kompaktes KPI-Set, ein Reifegrad-Prozessmodell sowie einen 180-Tage-Fahrplan übersetzt. Das Informationsmodell legt dafür fest, welche Daten je Gerät, Identität und Anwendung erhoben, wie sie qualitätsgesichert verdichtet und wann sie in Entscheidungen überführt werden; so entsteht ein prüffähiger Regelkreis, der Compliance-Anforderungen und Alltagstauglichkeit vereint.

1 BYOD zwischen Freiraum, Risiko und Steuerbarkeit

Der Beitrag ist bewusst als umsetzungsorientierter Fahrplan angelegt. Er vergleicht nicht sämtliche möglichen BYOD-Strategien im Sinne einer vollständigen Alternativenabwägung, sondern zeigt einen klaren Steuerungspfad: von Zielen über Daten und Kennzahlen hin zu Entscheidungen, Maßnahmen und Nachweisen. Die ausführlichere Herleitung der Modelllogik, insbesondere die Verbindung von Balanced Scorecard [Kaplan & Norton 1996], Informationsmodell und COBIT 19, ist in der zugrunde liegenden Arbeit breiter begründet [Groß 2025].

BYOD wird dabei nicht als modisches Einzelthema verstanden. Der Ansatz steht exemplarisch für eine breitere Herausforderung moderner IT-Governance: private, mobile und hybride Endpunkte greifen auf geschäftliche Anwendungen, Identitäten, Datenräume und Cloud-Dienste zu. Damit verschiebt sich die Steuerungsfrage von der reinen Geräteverwaltung hin zu kontrollierbaren Zugriffen, belastbaren Nachweisen und nachvollziehbaren Entscheidungen. Gerade deshalb eignet sich BYOD als kompaktes Anwendungsfeld, um zu zeigen, wie strategische Ziele, operative Kontrollen und prüffähige Evidenz miteinander verbunden werden können.

Viele Unternehmen erlauben die Nutzung privater Geräte. Gleichzeitig steigen die Anforderungen an Evidenz und Regelkonformität. Ohne klare Ziele, Messgrößen und eine Anbindung an Entscheidungen bleibt BYOD reaktiv. Wir verbinden die Logik der BSC, COBIT 19-Prozesse und ein Informationsmodell zu einem durchgängigen Steuerungsansatz. Eine empirische Studie mit über 1.000 Teilnehmenden zeigt Leistungszuwächse und einen Zusammenhang zur Ausrichtung an COBIT 19 [Groß 2025]. Einzelmaßnahmen – MDM-Profile, neue Richtlinien, App-Sperrlisten – lösen das Grundproblem nicht. Der Zielkonflikt bleibt: Mitarbeitende erwarten Reibungslosigkeit, Sicherheit verlangt Kontrolle, Compliance verlangt Evidenz. Wirksam wird BYOD erst, wenn diese Ziele in einen gemeinsamen Entscheidungsrahmen übersetzt werden. Dazu gehören ein knappes Regelwerk (Scope, Mindestanforderungen, Ausnahmen), wenige verlässliche Kennzahlen, die Entscheidungen auslösen, und routinierte Termine, in denen Abweichungen behandelt, Maßnahmen beschlossen und Wirkungen überprüft werden. So entsteht ein Regelkreis statt Ad-hoc-Aktionen.

Praxishebel sind: klar definierte Aufnahme- und Entzugsprozesse, sichtbare Zielwerte (z. B. Patch-Erfüllung, Onboarding-Zeit) sowie ein kurzer Entscheidungsrhythmus. Dann wird BYOD planbar und auditierbar – ohne die Nutzenden aus dem Blick zu verlieren.

2 BSC und COBIT 19 als Steuerungsrahmen

Die BSC verknüpft Fähigkeiten mit Prozessen, Nutzererlebnis und Finanzen. Für BYOD heißt das: Schulung und Onboarding-Hygiene (Fähigkeiten) stabilisieren Freigaben, Patching und Off/Onboarding (Prozesse). Das verbessert spürbar das Nutzererlebnis und stabilisiert Kosten/Nutzen. Entscheidend ist ein schlankes KPI-Set je Perspektive, das direkt eine Reaktion auslöst: Patch-Erfüllung und Onboarding-Zeit wirken auf Prozessqualität/Acceptance; Vorfallquote je 100 Geräte und Abschlussquote im Zieltermin halten Sicherheits- und Verbesserungsarbeit auf Kurs.

Kennzahlen sind kein Selbstzweck: Sie müssen Entscheidungen vorbereiten. Detailanalysen bleiben dort verortet, wo sie fachlich benötigt werden: im Betrieb, im Security-Monitoring oder im Servicemanagement. Das Lenkungsgremium benötigt dagegen verdichtete Entscheidungsinformationen: Zielwert erreicht oder verfehlt, Ursache plausibel erklärt, Maßnahme beschlossen, Wirkung überprüfbar. Dadurch bleibt die Steuerung schlank, ohne die fachliche Analyse zu verkürzen. COBIT 19 liefert klar definierte Rollen, Praktiken und Entscheidungspunkte, die die BSC-Logik im Alltag umsetzbar machen. Dafür genügen wenige, aber verbindliche Festlegungen: Wer gibt Anwendungen mit Begründung frei? Wer befristet Ausnahmen und überprüft sie? Wer beschließt Maßnahmen bei Abweichungen – und in welchem Rhythmus? Auf operativer Ebene unterstützt eine monatliche Lagebesprechung (Status, Abweichungen, Sofortmaßnahmen), auf strategischer Ebene ein quartalsweises Gremium (Zielwerte, Prioritäten, strukturelle Hemmnisse). Klar geregelte Eskalationspfade stellen sicher, dass rote Linien zeitnah Reaktionen auslösen [ISACA 2019a; ISACA 2019b].

So entstehen nachvollziehbare Beschlüsse mit messbarer Wirkung – ohne Mikromanagement. Das Ergebnis ist ein reproduzierbarer Regelkreis aus Messen, Entscheiden, Umsetzen und Überprüfen.

3 Informationsmodell: Welche Daten steuern BYOD?

Das Informationsmodell legt schlank und eindeutig fest, welche Informationen für BYOD benötigt werden, wo sie entstehen und wie sie zu entscheidungsreifen Berichten verdichtet werden. Im Zentrum stehen wenige, klar definierte Objekttypen: Geräte (Typ, Betriebssystemstand, Geräte-ID), Identitäten (Rolle, Bereich), Anwendungen (freigegeben oder geduldet, KI-Anteil), Datenklassen (personenbezogen, geschäftskritisch), Risiken (Eintrittswahrscheinlichkeit, Auswirkung), Kontrollen (Status, Wirksamkeit) sowie Ereignisse (Incident-Typ, Zeitstempel, Quelle). Für jedes Objekt werden Verantwortliche, Systemquellen (z. B. Mobile Device Management (MDM)/Mobile Application Management (MAM), Identity Provider (IdP), SecOps, IT-Finanzen), Aktualisierungskadenz (täglich, wöchentlich, monatlich) und Qualitätsregeln (Vollständigkeit, Eindeutigkeit, Plausibilität) festgelegt. Die Verdichtung erfolgt über schlanke Berichtsobjekte: Gerätebestand (Sichtbarkeit), Sicherheitslage (Patch-Erfüllung, Vorfallquote), Servicedurchlaufzeiten (On-/Offboarding, Abbau von Ausnahmen) und Ausnahmebestände (Begründung, Frist, Verantwortliche). Aus diesen Sichten werden Kennzahlen mit klarer Formel, Schwellenwert und Eskalationslogik abgeleitet, etwa »Patch-Compliance = gepatchte BYOD-Geräte / alle freigegebenen BYOD-Geräte« oder »Zeit bis Incident-Erstmeldung«. Jede Kennzahl verweist auf ihre Datenherkunft (Data Lineage) und löst bei Abweichungen automatisch Maßnahmen mit Owner und Termin aus – Berichte werden so zu verbindlichen Beschlüssen. Einheitliche Definitionen reduzieren Auslegungsspielräume, beschleunigen Prüfungen und sichern die Wiederholbarkeit von Entscheidungen [Groß 2025].

4 Relevante Regulierungen und Standards

Regulierungen und Standards dienen in diesem Beitrag nicht als vollständiger Rechtskommentar, sondern als Bezugspunkte für steuerbare Anforderungen. Ihre Relevanz hängt vom jeweiligen Organisationskontext ab: DORA (Digital Operational Resi-

lience Act) ist insbesondere für Finanzunternehmen einschlägig, NIS-2 für erfasste wesentliche und wichtige Einrichtungen, der EU AI Act für den Einsatz KI-basierter Anwendungen und ISO/IEC 27001 als internationaler Standard für Informationssicherheits-Managementsysteme. Für BYOD ist zusätzlich die Datenschutz-Grundverordnung (DSGVO) zentral, weil private Geräte im Dienstgebrauch personenbezogene Daten, Beschäftigtendaten, Nutzungsprotokolle, Kommunikationsinhalte oder geschäftliche Metadaten berühren können. Der regulatorische Kern besteht deshalb nicht darin, alle Vorgaben pauschal nebeneinanderzustellen. Entscheidend ist vielmehr, aus den jeweils einschlägigen Anforderungen konkrete Steuerungsfragen abzuleiten: Welche Geräte und Anwendungen sind zulässig, welche Daten werden verarbeitet, welche Nachweise entstehen, wer entscheidet bei Abweichungen und wie wird Wirksamkeit überprüft?

Die DSGVO nimmt in BYOD-Szenarien eine Querschnittsrolle ein. Private Geräte können dienstliche Daten aufnehmen oder zugänglich machen, ohne dass die Organisation private Inhalte unangemessen einsehen darf. Daraus entsteht ein besonders sensibler Steuerungspunkt: geschäftliche und private Daten müssen technisch und organisatorisch getrennt werden, Protokollierung und Monitoring benötigen Zweckbindung und Verhältnismäßigkeit, Zugriffe auf Unternehmensdaten brauchen klare Verantwortlichkeiten, und Lösch-, Sperr- sowie Offboarding-Prozesse müssen auch dann zuverlässig funktionieren, wenn das Endgerät nicht dem Unternehmen gehört. Für die IT-BSC bedeutet dies: Datenschutz ist keine nachgelagerte juristische Prüfung, sondern Teil von Scope, Datenmodell, Kontrolllogik und Kennzahlen. Messbar werden etwa Vollständigkeit der Gerätezuordnung, Anteil freigegebener Anwendungen, dokumentierte Ausnahmen, fristgerechte Lösch- und Entzugsprozesse sowie die Qualität der Nachweise.

DORA ist kein allgemeiner BYOD-Standard für alle Organisationen, sondern ein sektorspezifischer Bezugspunkt für Finanzunternehmen und deren IKT-Risikomanagement. Gerade dort zeigt sich aber besonders klar, welche Anforderungen an operative Resilienz, Nachvollziehbarkeit und Reaktionsfähigkeit auch für BYOD relevant werden können. Sobald private Endgeräte auf geschäftskritische Anwendungen, Kundendaten, Cloud-Dienste oder ausgelagerte IKT-Leistungen zugreifen, müssen Risiken auf Geräte-, Identitäts- und Prozessebene steuerbar sein. Praktisch bedeutet das: BYOD-Freigaben sollten an Mindestkontrollen gebunden werden, Incidents benötigen belastbare Zeitstempel und eindeutige Geräte-/Identitätsbezüge, Tests müssen realistische Nutzungsszenarien berücksichtigen, und Mobile-, Identity- oder Cloud-Provider sind in die Dienstleistersteuerung einzubinden. In der IT-BSC zahlen diese Anforderungen vor allem auf Prozessqualität, Resilienz und Lernfähigkeit ein; geeignete Kennzahlen sind etwa Patch-Erfüllung, mobile Vorfallquote, Zeit bis Erstmeldung, Testabdeckung und Umsetzungsgrad offener Maßnahmen. COBIT 19 liefert dafür Prozessanker, etwa für Sicherheitsservices, Lieferantenmanagement und Überwachung.

NIS-2 ist ebenfalls nicht für jede Organisation gleichermaßen einschlägig, verdeutlicht aber einen breiteren Steuerungsmaßstab: Cybersicherheitsmaßnahmen müssen risikobasiert, angemessen, nachvollziehbar und organisatorisch verankert sein. Der Begriff »angemessen« ist dabei nicht als Unschärfe zu verstehen, sondern als Ausdruck prinzipienbasierter Regulierung mit Bewertungsspielraum. Für BYOD lässt sich dieser Maßstab in konkrete Anforderungen übersetzen: Geräte dürfen nicht anonym oder außerhalb definierter Mindeststandards betrieben werden, Zugriffe sollten an Identität, Rolle, Gerätezustand und Kontext gebunden sein, Ausnahmen müssen befristet und begründet werden, und Sicherheitsereignisse müssen so dokumentiert sein, dass Melde- und Eskalationswege funktionieren. In der IT-BSC können daraus Zielwerte für Onboarding-Durchlaufzeiten, Ausnahmebestände, Geräte-Health-Checks, Schulungsabdeckung und Lieferkettenbezug entstehen. Der Nutzen liegt darin, dass BYOD nicht nur als technische Freigabe behandelt wird, sondern als wiederkehrender Managementprozess mit klaren Verantwortlichkeiten.

Der EU AI Act wird für BYOD besonders relevant, wenn auf privaten oder mobilen Endgeräten KI-basierte Anwendungen genutzt werden. Dabei geht es nicht nur um die KI-Anwendung selbst, sondern auch um Datenflüsse, Protokollierung, Nutzungsgrenzen und die Verbindung zur DSGVO. Im BYOD-Katalog sollte deshalb je Anwendung erkennbar sein, ob eine KI-Komponente enthalten ist, welche Datenarten verarbeitet werden, ob personenbezogene oder geschäftskritische Informationen betroffen sind und welche Nutzungsgrenzen gelten. Praktikable Kontrollen sind etwa eine Liste freigegebener KI-Anwendungen, Vorgaben zur Verarbeitung sensibler Inhalte, Speicher- und Weitergaberegeln, Prompt- und Output-Poli-

Perspektive	Governance-Ziel (COBIT 19)	Beispiel-KPI	Datenquelle	Frequenz
Finanzen	**EDM03** – Stakeholder-Transparenz	TCO je BYOD-Nutzer	Controlling, IT-Finanzen	Quartal
Nutzer	**APO08** – Beziehungsmanagement	Zufriedenheit (Score)	Kurzumfrage	Halbjahr
Prozesse	**DSS05** – Sicherheitsservices	Vorfallquote je 100 Geräte	SecOps-Monitoring	Monat
Prozesse	**DSS01** – Betriebsleistungen	Patch-Compliance (%)	Endpoint-Management	Woche
Lernen & Entwicklung	**MEA01** – Leistungs-Monitoring	Offene Audit-Feststellungen	Audit-Tool	Quartal

Tab. 1: Entscheidungsorientiertes KPI-Set für BYOD

cies sowie rollenspezifische Schulungen. In der IT-BSC lassen sich daraus Kennzahlen ableiten, etwa der Anteil freigegebener gegenüber erkannter KI-Apps, Policy-Verstöße je 100 Geräte, Schulungsabdeckung pro Rolle oder die Zahl offener Klärungen zu risikorelevanten Anwendungen. Dadurch wird KI-Nutzung nicht pauschal blockiert, sondern kontrolliert, dokumentiert und in verantwortbare Bahnen gelenkt.

ISO/IEC 27001 schafft schließlich den Managementsystemrahmen, um Anforderungen aus Datenschutz, Cybersicherheit, Resilienz und KI-Governance in konkrete Richtlinien, Kontrollen, Nachweise und Verbesserungsroutinen zu übersetzen. Für BYOD sind insbesondere Regelungen zu Rollen und Verantwortlichkeiten, Asset- und Zugriffsteuerung, Gerätekonfiguration, Protokollierung, Lieferantenbezug, Incident-Management und Compliance relevant. Der praktische Wert liegt darin, dass einzelne Maßnahmen nicht isoliert stehen bleiben: Mindeststandards werden dokumentiert, Risiken bewertet, Kontrollen zugeordnet, Abweichungen behandelt, Maßnahmen nachverfolgt und die Wirksamkeit regelmäßig überprüft. Die IT-BSC macht diese Managementsystemlogik entscheidungsfähig, indem sie Zielwerte und Abweichungen verdichtet; COBIT 19 ergänzt Rollen, Praktiken und Entscheidungspunkte. So entsteht ein belastbarer Regelkreis, der nicht nur Regelkonformität behauptet, sondern sie über Daten, Kontrollen und Managemententscheidungen nachvollziehbar macht.

Im Gesamtbild liefern DSGVO, DORA, NIS-2, EU AI Act und ISO/IEC 27001 also keine starre Pflichtliste, sondern unterschiedliche Perspektiven auf dasselbe Steuerungsproblem. Datenschutz fragt nach Rechtmäßigkeit, Zweckbindung und Trennung privater und geschäftlicher Sphären. DORA [EU 2022a] betont operative Resilienz und Nachweisfähigkeit im Finanzsektor. NIS-2 [EU 2022b] stärkt risikobasierte Cybersicherheitsmaßnahmen und Meldewege für betroffene Einrichtungen. Der EU AI Act [EU 2024] ergänzt Anforderungen an KI-bezogene Nutzung, Transparenz und Daten-Governance. ISO/IEC 27001 [ISO 2022] macht diese Anforderungen in einem prüfbaren Managementsystem bearbeitbar. Für IT-Manager ergibt sich daraus ein pragmatisches Vorgehen: Scope festlegen, zulässige Geräte und Anwendungen definieren, Datenklassen und Rollen zuordnen, wenige entscheidungsfähige Kennzahlen bestimmen, Zielwerte setzen und eine feste Kadenz etablieren, in der Abweichungen zu Maßnahmen, Verantwortlichen und Fristen führen. Genau dort verbinden IT-BSC und COBIT 19 regulatorische Anforderungen mit operativer Steuerbarkeit.

5 KPI-Set: von der Perspektive zur Entscheidung

Messlogik und Formeln: Für die Patch-Compliance werden alle BYOD-Geräte mit verwalteter Telemetrie als Nenner herangezogen; die Quote ist der Anteil der Geräte, die innerhalb des definierten Servicefensters den Soll-Patch-Stand erreicht haben. Für die Onboarding-Zeit zählt die Spanne vom Antrag bis zur ersten produktiven Nutzung (Median als robuste Kennzahl). Die Vorfallquote bezieht sich auf bestätigte, sicherheitsrelevante Ereignisse je 100 Geräte pro Monat.

Zielwerte und Toleranzen: Ein praxistauglicher Startpunkt liegt bei Patch-Compliance ≥ 95 %, Onboarding-Zeit ≤ 3 Arbeitstage und Vorfallquote ≤ 1,0/100 Geräte/Monat. Toleranzen (z. B. −2 Prozentpunkte bzw. +1 Tag) sind erlaubt, müssen aber spätestens im nächsten Quartalsgremium mit Maßnahmen hinterlegt werden.

Datenquellen und Qualität: Patch-Status aus der Endgeräteverwaltung, Onboarding aus dem Servicemanagement, Vorfälle aus dem Security-Monitoring, Zufriedenheit aus einer 2-Minuten-Kurzumfrage. Jede Quelle besitzt einen Owner sowie einen Aktualisierungszyklus (wöchentlich/monatlich). Fehlerlisten werden im 14-Tage-Takt abgearbeitet.

Entscheidungslogik (Wenn-dann-Regeln): Wird ein Zielwert in zwei aufeinanderfolgenden Messpunkten verfehlt, erfolgt eine Ursachenanalyse binnen zehn Arbeitstagen; anschließend wird eine Maßnahme mit Termin und Verantwortlichen beschlossen. Drei Messpunkte außerhalb der Toleranz lösen eine Eskalation ins Gremium aus.

Dashboard und Visualisierung: Eine Seite genügt – Ampeln je KPI, Trend über sechs Monate, Top-3-Ursachen, zwei offene Maßnahmen mit Fälligkeit. Drill-downs bleiben in den Fachwerkzeugen; Führung sieht nur Entscheidungsinformationen.

Rollen und RACI: IT-Betrieb verantwortet Patch-KPI, Service-Owner die Onboarding-Zeit, SecOps die Vorfallquote, die IT-Governance orchestriert das Dashboard. Fachbereiche liefern Feedback für die Zufriedenheitsmessung, HR (Human Resources) unterstützt mit Schulungsquote und Starter-Journeys.

6 Reifegrad der BYOD-Steuerung

Der Reifegrad ist ein Prozess von Sichtbarmachen → Regeln → Standardisieren → Steuern → Verbessern.

Level	Merkmale	Nächste Schritte
1 – Ad hoc	Duldung; geringe Sichtbarkeit	Policy; Minimal-Kontrollen
2 – Definiert	Regeln; uneinheitliche Umsetzung	Standardisierung; Datenqualität
3 – Etabliert	Konsistente Prozesse; Reporting	Zielwerte; Eskalation
4 – Gesteuert	Datenbasierte Entscheidungen	Automatisierung; Lieferkette
5 – Optimiert	KVP; BYOD als Enabler	Benchmarks; Innovation

Tab. 2: Reifegrad – Merkmale und nächste Schritte

Bewertungssystem: Jede der fünf Stufen wird entlang von sechs Dimensionen beurteilt – Sichtbarkeit, Standardisierung, Datenqualität, Entscheidungsroutinen, Automatisierung, Audit-Readiness. Pro Dimension wird auf einer Skala von 1 bis 5 bewertet; der Reifegrad ist das gerundete Mittel, die schwächste Dimension erhält einen speziellen Fokus im Verbesserungsplan.

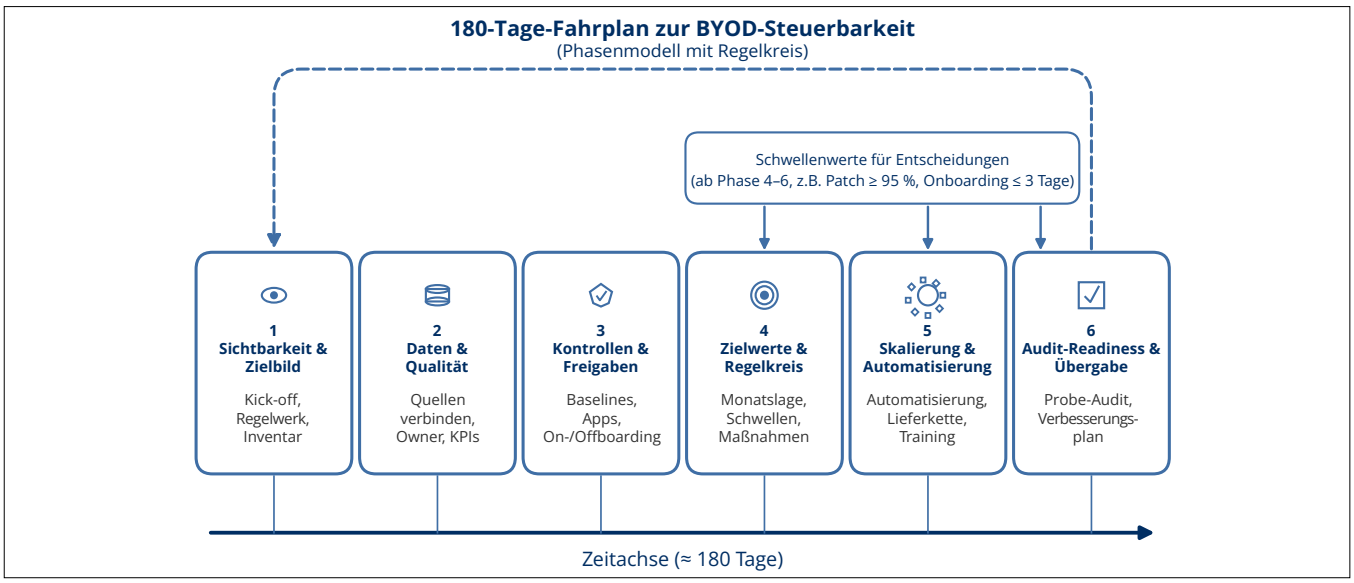

Abb. 1: 180-Tage-Fahrplan

Evidenzbasierte Kriterien je Stufe: Level 2 erfordert mindestens definierte Mindeststandards (z. B. Verschlüsselung, Sperrrichtlinie) und einen dokumentierten Ausnahmeprozess; Level 3 verlangt konsistente Umsetzung und ein monatliches Reporting; Level 4 fordert messbare Entscheidungen mit Wenn-dann-Regeln; Level 5 weist automatisierte Kontrollen, Lieferketten-Sicht und einen jährlichen Verbesserungszyklus nach.

Assessment-Vorgehen: Zwei Workshops (je 90 Minuten) mit IT-Betrieb, SecOps, Servicemanagement, Governance und einem Vertreter der Fachbereiche. Vorab werden Telemetriedaten und Richtlinien gesichtet. Ergebnis ist ein Reifegradprofil mit drei priorisierten Lücken und einem 12-Monats-Plan.

Übergang zwischen Stufen: Von 2 → 3 steht Standardisierung im Fokus (Vorlagen, Self-Service, Datenwege); von 3 → 4 werden Zielwerte und Eskalationspfade verbindlich gemacht; von 4 → 5 richtet Automatisierung und Lieferkette aus. Anti-Regression: Quartalsweise Stichproben prüfen, ob erreichte Praktiken beibehalten werden.

7 180-Tage-Fahrplan: vom Start zur nachhaltigen Steuerbarkeit

Der 180-Tage-Fahrplan ist ein abrollender Regelkreis. Jede Phase liefert greifbare Ergebnisse und bereitet die nächste vor: **1** Sichtbarkeit & Zielbild, **2** Daten & Qualität, **3** Kontrollen & Freigaben, **4** Zielwerte & Regelkreis, **5** Skalierung & Automatisierung, **6** Audit-Readiness & Übergabe. Entscheidungen folgen klaren Schwellenwerten; Nachweise entstehen aus dem Arbeiten heraus.

Tage 1–30 – Sichtbarkeit & Zielbild: Stakeholder klären Zweck, Geltungsbereich und Erwartungen in einem 60-Minuten-Kick-off. Ein leichtgewichtiges Regelwerk (max. zwei Seiten) beschreibt Mindeststandards, Freigaben und befristete Ausnahmen. Das erste Inventar wird aus Endgeräteverwaltung, Identitäten und Servicemanagement zusammengeführt; fehlende Felder (z. B. Besitzer, letzter Patch-Stand) werden markiert. Die Onboarding-Kette wird als Swimlane modelliert; Engpässe (z. B. manuelle Freigaben) erhalten Sofortmaßnahmen.

Tage 31–60 – Daten & Qualität: Vier Datenquellen werden technisch verbunden (Endgeräte, Identity and Access Management (IAM), SecOps-Monitoring, Servicemanagement). Für jedes Kernfeld wird ein Owner mit Aktualisierungszyklus benannt. Eine 14-tägige Fehlerliste räumt doppelte/alte Einträge auf. Das erste Dashboard zeigt die drei Kern-KPIs mit Trend und Ampelfarben; Zielwerte werden fachlich verprobt und in der Leitung bestätigt.

Tage 61–90 – Kontrollen & Freigaben: Mindeststandards (Verschlüsselung, Bildschirmsperre, Betriebssystemstand) werden als maschinenlesbare Baselines umgesetzt. Eine App-Freigabeliste dokumentiert Zweck, Datenarten und Verantwortliche; Ausnahmen sind befristet und werden automatisch erinnert. Self-Service-Onboarding und ein klarer Offboarding-Pfad reduzieren Ticketaufkommen und verkürzen Durchlaufzeiten.

Tage 91–120 – Zielwerte & Regelkreis: Die monatliche Lage ist etabliert; das quartalsweise Gremium setzt verbindliche Zielwerte (Patch ≥ 95 %, Onboarding ≤ 3 Tage, Vorfallquote unter Schwelle). Jede Abweichung löst eine Maßnahme mit Termin und Owner aus; die Wirkung wird im nächsten Termin überprüft. Das Dashboard zeigt zusätzlich Zufriedenheit und offene Audit-Feststellungen.

Tage 121–150 – Skalierung & Automatisierung: Erinnerungen und Sperrgründe werden automatisiert; Offboarding wird als Standardprozess in HR-Journeys verankert. Die Lieferkette wird über Anbieterbewertungen und Vertragsklauseln einbezogen (Telemetrie-Mindestdatensatz, Reaktionszeiten). Schulungsmodule (20-Minuten-Mikro-Learning) für Starter und BYOD-Wechsler werden ausgerollt.

Tage 151–180 – Audit-Readiness & Übergabe: Ein Probe-Audit prüft Wirksamkeit und Nachweisführung. Offene Punkte erhalten Fristen; ein 12-Monats-Verbesserungsplan wird verabschiedet. Der Regelbetrieb überführt den Fahrplan in eine wiederkehrende Kadenz mit zwei Verbesserungswellen pro Jahr. Ergebnis: BYOD ist messbar, nachvollziehbar und akzeptiert.

8 Typische Fallstricke und Fazit

Priorisierung statt Aktionismus: Werden Zielwerte verfehlt, entscheidet die Schwere des Risikos und die Betroffenheit über die Reihenfolge der Maßnahmen. Hohe Auswirkung und hohe Eintrittswahrscheinlichkeit kommen zuerst; der Rest wird terminiert – nicht alles wird parallel gestartet. Jede Maßnahme erhält Scope, Owner, Start/Ende und ein messbares Ergebnis (z. B. +5 Prozentpunkte Patch-Erfüllung binnen zwei Wochen). Die Wirkung wird im nächsten Termin überprüft; wird kein Effekt erzielt, wird nachgeschärft oder gestoppt.

Kommunikation als Kontrollwirkung: Kurze Hinweise am Point of Action (Self-Service-Portal, Onboarding-Schritte, Servicekatalog) verhindern Fehlkonfigurationen besser als lange Richtlinien. Mini-FAQs zu Freigaben, Ausnahmen und Offboarding senken Ticketaufkommen und Eskalationen.

Lieferkette gezielt einbinden: Externe Apps/Dienstleister erhalten gleiche Zielwerte (Patch-Zyklus, Reaktionszeit). Ein Telemetrie-Mindestdatensatz (Version, Patch-Stand, Vorfallsignal) zeigt Risiken früh; Verstöße führen zu abgestuften Reaktionen.

Frühindikatoren nutzen: Trendbrüche bei Vorfallquote, Patch-Erfüllung oder Onboarding-Zeit werden wöchentlich gescreent. Eine einfache Heuristik (drei Messpunkte nacheinander außerhalb der Toleranz) reicht, um zwischen den Quartalsterminen zu handeln. Routinen schlagen Ad-hoc-Maßnahmen: Eine feste Kadenz (monatliche Lage, quartalsweise Entscheidungen) verhindert stille Erosion. Jede Abweichung erhält Owner und Enddatum und wird im Folgetermin nachgehalten [EU 2022a; EU 2022b; ISO 2022]. BYOD zahlt sich aus, wenn Kennzahlen nicht isoliert berichtet, sondern unmittelbar in Entscheidungen, Maßnahmen und Wirksamkeitsprüfungen überführt werden. Jede Zahl braucht Bedeutung, jede Abweichung eine Reaktion, jeder Beschluss einen Nachweis der Wirkung. So werden Lern- und Steuerungsschleifen kurz, und Investitionen in Automatisierung oder Schulung wirken schneller. Kulturell gelingt BYOD, wenn Fairness spürbar ist: klare Regeln, knappe Begründungen, nachvollziehbare Ausnahmen. Führung kommuniziert sichtbar, warum eine Maßnahme getroffen oder verworfen wird – das steigert Akzeptanz und reduziert die Schatten-IT.

Technisch reichen robuste Identitäten, saubere Gerätekonfigurationen, verlässliche Telemetrie und klar getrennte Datenklassen. Alles andere ist Orchestrierung im Regelkreis – COBIT 19 liefert Struktur und Disziplin, die IT-BSC die Ziel-/Kennzahl-Übersetzung. Regulatorisch wird Compliance zum Nebenprodukt eines funktionierenden Systems: BYOD-Sichten im Risikoregister, geübte Meldewege, geprüfte Kontrollen, dokumentierte Zielwerte, Probe-Audit mit Abstellplan – genau die Evidenz, die DORA, NIS-2, AI Act und ISO/IEC 27001 verlangen.

9 Ausblick

Der 180-Tage-Fahrplan etabliert das Minimum-Viable-Governance-System. Danach hält ein jährlicher Verbesserungsplan das Tempo: zwei Releases, gezielte Automatisierungen, Review der Zielwerte und eine kurze Wirksamkeitsprüfung. So bleibt BYOD dauerhaft steuerbar, auditierbar – und beliebt bei Nutzenden.

Literatur

[EU 2022a] *Europäische Union (EU):* Verordnung (EU) 2022/2554 über die digitale operationelle Resilienz (DORA), 2022.

[EU 2022b] *Europäische Union (EU):* Richtlinie (EU) 2022/2555 über ein hohes gemeinsames Cybersicherheitsniveau (NIS-2), 2022.

[EU 2024] *Europäisches Parlament und Rat:* Gesetz über Künstliche Intelligenz (AI Act), 2024.

[Groß 2025] *Groß, M.:* Information model in the system for measuring and managing the performance of the balanced scorecard. Dissertation, 2025.

[ISACA 2019a] *ISACA:* COBIT® 2019 Framework – Introduction & Methodology. ISACA, 2019.

[ISACA 2019b] *ISACA:* COBIT® 2019 Governance and Management Objectives. ISACA, 2019.

[ISO 2022] ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements, 2022.

[Kaplan & Norton 1996] *Kaplan, R.; Norton, D.:* The Balanced Scorecard. Harvard Business School Press, Boston, 1996.

Markus Groß

ist langjähriger Experte für IT-Governance, Informationssicherheit und Regulatorik. Er konzipiert und prüft Steuerungs- und Kontrollrahmen auf Basis anerkannter IT-Governance- und Sicherheitsstandards und übersetzt aktuelle regulatorische Anforderungen in messbare KPI/KRI-Systeme, belastbare Nachweise und auditsichere Entscheidungsprozesse.

Dr. Markus Groß
Carl-Langhans-Str. 8
40789 Monheim am Rhein
kontakt@markusgross.de
www.markusgross.de