SECURITY & COMPLIANCE

Purview Insider Risk Management: Alert-Klassifizierung ersetzt bisherige Dismiss-Gründe

Consulting Briefing · 27.11.2026 · boddenberg.de

Executive Summary

Bisher konntest du einen Insider-Alert nur auf eine Art begründen: indem du ihn wegwirfst. Laut Microsoft-Ankündigung MC1568697 bekommt Microsoft Purview Insider Risk Management (IRM) eine eigene Alert-Klassifizierung mit drei Werten: True positive, Benign positive und False positive, jeweils mit einer vordefinierten Begründung. Die bisherigen Dismiss-Gründe fallen dafür weg. Das ist eine Abkündigung, auch wenn Microsoft sie in der Meldung in einem einzigen Nebensatz versteckt.

Die Public Preview startet Anfang Dezember 2026, der weltweite Rollout beginnt Mitte Januar 2027 und soll Ende Januar abgeschlossen sein. Konfigurieren musst du nichts. Vorbereiten musst du trotzdem einiges: einen Leitfaden, wann welches Etikett gilt, eine Schulung für Analysten und Ermittler, angepasste Reports und ein Gespräch mit Betriebs- oder Personalrat. Denn das neue Feld schreibt künftig ausdrücklich an einen Vorgang über einen Beschäftigten: „Hier war ein echtes Risiko." Das ist kein Kosmetik-Update, das ist ein Stempel.

Fakten: Das Wichtigste auf einen Blick

Quelle: Microsoft-Ankündigung MC1568697, Stand 26.11.2026, Roadmap-Eintrag 576710. Betroffener Dienst: Microsoft Purview Insider Risk Management.

Was wegfällt: die Dismiss-Gründe beim Verwerfen eines Alerts. Die Aktionen Confirm und Dismiss wandern unter eine neue Aktion „Manage".

Was neu kommt: die Aktion „Classify" und eine Spalte „Classification" in der Alert-Warteschlange, unabhängig vom Status.

Termine: Preview Anfang bis Mitte Dezember 2026, global Mitte bis Ende Januar 2027, Meldung läuft bis 29.03.2027. Dringlichkeit: mittel, Vorbereitung bis Mitte Januar.

Worum geht es im Detail?

Kurz zur Erinnerung, was IRM eigentlich tut. Insider Risk Management korreliert Signale aus Microsoft 365, Endpunkten und HR-Konnektoren und schlägt an, wenn jemand sich riskant verhält: der Vertriebler, der drei Wochen vor seinem letzten Arbeitstag die Kundendatenbank auf einen USB-Stick zieht, die Entwicklerin, die Quellcode in ein privates Cloud-Konto kopiert, oder der Kollege, der vertrauliche Präsentationen an seine private Adresse mailt. Die Benutzernamen sind standardmäßig pseudonymisiert, der Zugriff hängt an eigenen Rollengruppen für Analysten und Ermittler, und alles landet im Audit-Log. Microsoft nennt das „Privacy by Design". Wir nennen es die Mindestausstattung, ohne die in Deutschland kein Betriebsrat auch nur den Raum betreten würde.

Jeder Alert hat einen Workflow-Status: Needs review, Confirmed, Dismissed oder Resolved. Laut Microsoft Learn bleiben Alerts im Status Needs review 120 Tage erhalten und werden dann gelöscht, aktive Fälle dagegen unbegrenzt. Wer einen Alert bisher verwarf, wählte einen Grund aus einer kurzen Liste. Die las sich ungefähr so: „Aktivität ist für diesen Benutzer erwartet“, „Zu viele Aktivitäten für diesen Benutzer“ und, kein Witz, „Aktivität ist wichtig genug, um weiter zu ermitteln“ als Grund fürs Verwerfen. Das Feld hatte also zwei Konstruktionsfehler: Es gab eine Begründung nur für das Wegklicken, und es vermischte Ergebnis, Bauchgefühl und Arbeitsorganisation.

Was sich ändert: aus einem Feld werden zwei Achsen. Der Status beschreibt künftig nur noch, wo der Alert im Prozess steht. Die Klassifizierung beschreibt, was er inhaltlich war. Beide sind laut Meldung voneinander entkoppelt: Ein Statuswechsel überschreibt die Klassifizierung nicht, und eine neue Klassifizierung ändert den Status nicht. Ein Alert kann also „Dismissed“ und gleichzeitig „True positive“ sein, etwa weil das Risiko echt war, aber schon über einen anderen Fall bearbeitet wird.

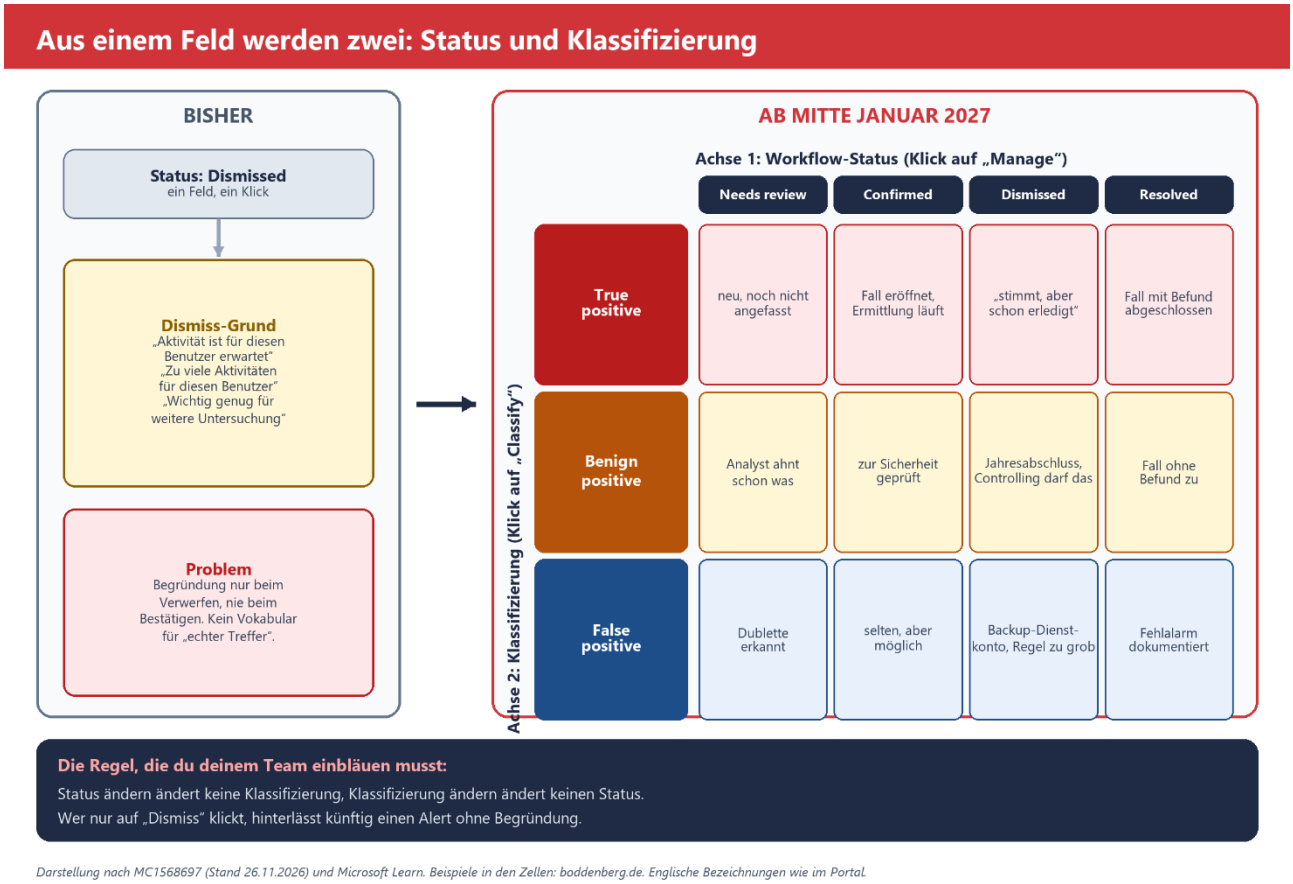

Abbildung 1: Status und Klassifizierung sind künftig zwei unabhängige Achsen. Jede Kombination ist möglich, auch die seltsamen.

Der eigentliche Grund steht zwischen den Zeilen: Defender. Microsoft Defender XDR kennt diese drei Klassen seit Jahren. Seit IRM-Alerts auch im Defender-Portal auftauchen, hatte ein und derselbe Alert zwei Wahrheiten, je nachdem, in welchem Portal man ihn anfasste. Die Meldung sagt es offen: Es geht um konsistente Klassifizierung für Alerts, die Purview und Defender teilen. Das ist die Harmonisierung zweier Welten, und dein SOC wird sie begrüßen, weil es endlich eine gemeinsame Sprache für Trefferquoten gibt.

Wichtig: Microsoft kann sich nicht entscheiden, wie die mittlere Klasse heißt

In derselben Meldung heißt der mittlere Wert einmal „Benign (operational)“, einmal „Benign Positive“ und in den Empfehlungen „Informational, expected activity“, so wie in Defender. Gemeint ist immer dasselbe: Die Aktivität hat stattgefunden, war aber erlaubt oder für die Rolle normal. Schreib deinen Leitfaden mit der Bezeichnung, die nach dem Rollout tatsächlich in deinem Portal steht, und nicht mit der aus der Meldung. Sonst diskutiert dein Team im Februar über Wörter statt über Risiken.

Klassifizierung	Bedeutung laut Microsoft	Typisches Beispiel aus der Praxis
True positive	Aktivität fand statt und stellt ein relevantes Geschäftsrisiko dar	Gekündigter Key-Account-Manager lädt 4.000 Angebote herunter
Benign positive	Aktivität fand statt, war aber autorisiert oder rollentypisch	Controlling exportiert zum Jahresabschluss die halbe Finanzablage
False positive	Alert bildet Aktivität oder Risiko nicht korrekt ab	Dublette, Backup-Dienstkonto, falsch zugeordnete Aktivität, zu grobe Schwelle

Was sind Chancen? Was sind Risiken?

Die Chance heißt Tuning mit Zahlen statt mit Gefühl. Jeder IRM-Admin kennt die Frage aus der Geschäftsführung: „Bringt das Ding überhaupt was?“ Bisher war die ehrliche Antwort ein Schulterzucken, denn verworfene Alerts sagten nichts darüber, ob die Richtlinie zu scharf, zu lasch oder einfach falsch zugeschnitten war. Mit einer sauberen Klassifizierung kannst du pro Richtlinie die False-Positive-Quote ausweisen und Schwellen gezielt nachjustieren. Viele Benign positives aus dem Controlling? Dann gehört das Controlling in eine Ausnahmegruppe. Viele False positives durch ein Dienstkonto? Ausschließen. Das spart Analystenzeit, und Analystenzeit ist in IRM das, was am schnellsten ausgeht, gleich nach dem Verständnis des Betriebsrats.

Das Risiko heißt Etikett mit Langzeitwirkung. „True positive“ ist eine dokumentierte Feststellung, dass ein bestimmter Mensch ein relevantes Geschäftsrisiko verursacht hat. Das ist arbeitsrechtlich heikel, weil so ein Vermerk später in einer Abmahnung oder einem Kündigungsschutzprozess auftauchen kann. Und datenschutzrechtlich, weil Art. 5 DSGVO verlangt, dass solche Daten richtig sind. Ein Analyst, der freitags um 17 Uhr aus Frust alles als True positive markiert, erzeugt keine Sicherheit, sondern Haftung.

Warnung: Der Praktikant, der zum Datendieb wurde

Ein Maschinenbauer hatte IRM ein halbes Jahr im Einsatz, als ein Praktikant im Abschlussmonat Hunderte CAD-Dateien in sein OneDrive synchronisierte. Großalarm, Fall eröffnet, Abteilungsleiter informiert. Ergebnis: Der Betreuer hatte ihn angewiesen, die Zeichnungen für die Abschlussarbeit zusammenzutragen. Im alten Modell wurde der Alert verworfen, und niemand wusste später mehr, warum. Im neuen Modell gehört da „Benign positive“ samt Begründung dran, und zwar nicht „True positive“, nur weil der Fall schon eröffnet war. Sonst steht der junge Mann in deiner Statistik für immer neben dem echten Spion vom letzten Jahr. Das ist das Schöne an Daten: Sie vergessen nie, sie verzeihen nur nicht.

Mitbestimmung: Ja, das gehört auf den Tisch. IRM selbst ist eine technische Einrichtung, die zur Überwachung von Verhalten und Leistung geeignet ist, sogar dafür gebaut. Damit greift § 87 Abs. 1 Nr. 6 BetrVG, bei Bundesbehörden § 80 Abs. 1 Nr. 21 BPersVG, in den Ländern das jeweilige Landespersonalvertretungsrecht. Wer IRM produktiv betreibt, hat hoffentlich eine Betriebs- oder Dienstvereinbarung. Die Frage ist, ob die neue Klassifizierung davon gedeckt ist. Sie ist es nicht automatisch, denn sie bringt eine neue Bewertungskategorie und eine neue Auswertungsmöglichkeit: Reports über Trefferquoten lassen sich nach Abteilungen schneiden, und dann sieht man plötzlich, welches Team „die meisten echten Fälle“ hat.

Vor dem Rollout solltest du mit dem Gremium deshalb vier Dinge klären: welche Klassifizierungen es gibt und nach welchen Kriterien sie vergeben werden, wer klassifizieren und wer die Klassifizierung sehen darf, ob und auf welcher Ebene Auswertungen erlaubt sind (Richtlinie ja, Person oder Kleinteam nein) und was mit der Klassifizierung passiert, wenn ein Fall gelöscht wird. Bilden Leitfaden und Vereinbarung das sauber ab, reicht oft eine Ergänzung der Anlage. Fehlen diese Regeln ganz, brauchst du vor Mitte Januar eine Zustimmung. Der Datenschutzbeauftragte passt parallel das Verzeichnis der Verarbeitungstätigkeiten und die Datenschutz-Folgenabschätzung an, die es für IRM ohnehin geben muss.

Aspekt	Chance	Risiko	Priorität
Sicherheit	messbare Trefferquote, gezieltes Tuning	Alerts ohne Begründung, wenn nur „Manage“ geklickt wird	hoch
Datenschutz	nachvollziehbare, begründete Entscheidungen	falsche True-positive-Etiketten, Art. 5 DSGVO	hoch
Mitbestimmung	Anlass, Bewertungskriterien sauber zu regeln	neue Auswertung ohne Deckung durch die Vereinbarung	hoch
Betrieb	gemeinsame Sprache mit Defender und SOC	Reports und Exporte auf alte Dismiss-Gründe brechen	mittel
Lizenzen	keine Zusatzkosten, Teil von IRM	keine, sofern IRM bereits lizenziert ist	niedrig

Zur Lizenz kurz und schmerzlos: Die Klassifizierung kostet nichts extra. Sie steckt in Insider Risk Management, und IRM brauchst du ohnehin über Microsoft 365 E5, A5 oder G5, E5 Compliance

oder das passende Add-on. Wer IRM nicht lizenziert hat, kann diesen Artikel als Gute-Nacht-Geschichte lesen.

Was müssen wir jetzt schon vorbereiten?

Microsoft schreibt: „No configuration changes are required." Das stimmt technisch, und es ist trotzdem der gefährlichste Satz der Meldung. Denn ohne Vorbereitung klicken deine Analysten ab Mitte Januar auf „Manage", finden ihren gewohnten Dismiss-Grund nicht mehr und verwerfen den Alert einfach ohne Klassifizierung. Dann hast du statt schlechter Begründungen gar keine.

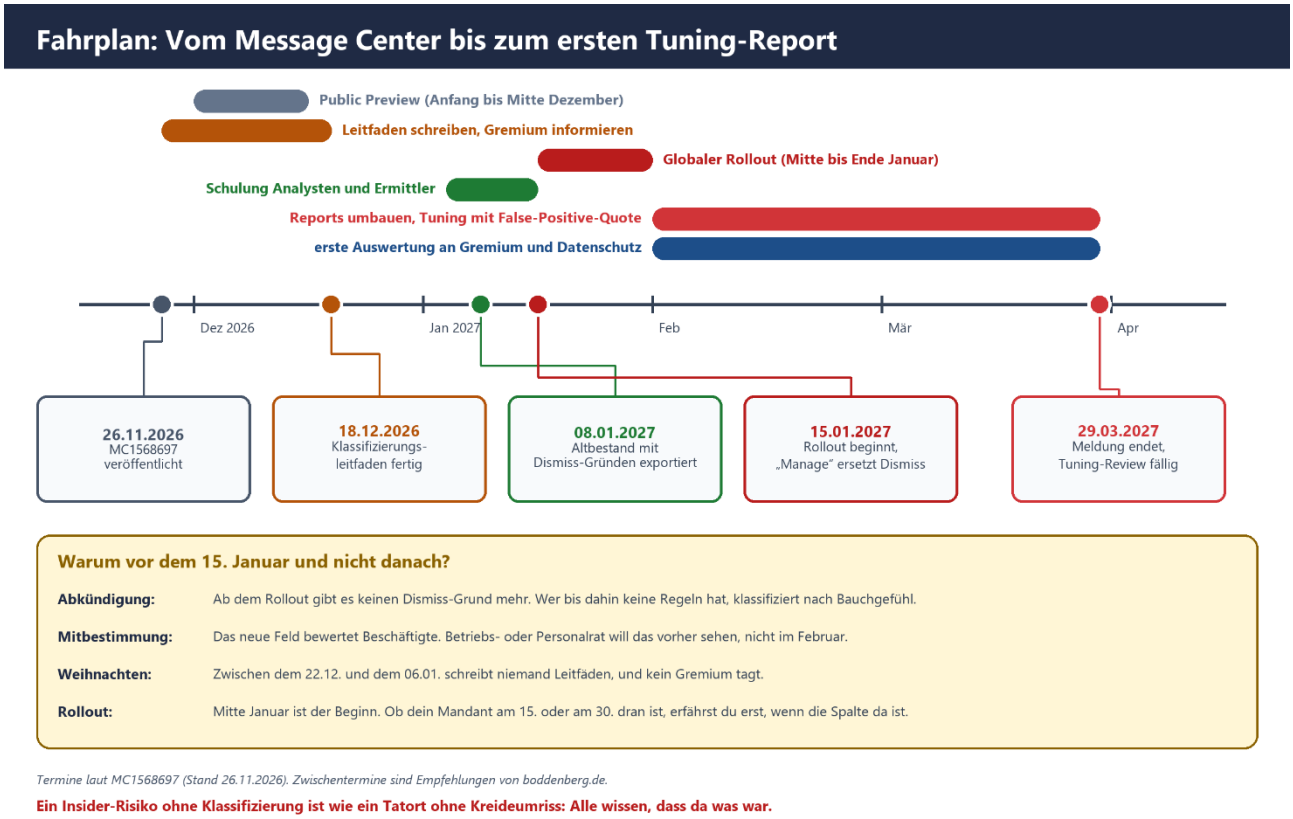

Abbildung 2: Der Rollout kommt Mitte Januar, dein Leitfaden sollte vor Weihnachten fertig sein.

Bisheriger Dismiss-Grund	Naheliegende neue Klasse	Hinweis für deinen Leitfaden
„Aktivität ist für diesen Benutzer erwartet"	Benign positive	passt fast eins zu eins, Begründung „rollentypisch" oder „autorisiert"
„Zu viele Aktivitäten für diesen Benutzer"	meist False positive	eigentlich ein Tuning-Signal: Schwelle zu grob, Richtlinie prüfen
„Wichtig genug, um weiter zu ermitteln"	keine Entsprechung	gehört nicht zum Verwerfen, sondern zu Confirm und Fall

Tipp: Altbestand sichern, bevor er seine Begründung verliert

Die Meldung sagt nicht, was mit den Dismiss-Gründen bereits verworfener Alerts passiert. Verlass dich nicht darauf, dass sie sichtbar bleiben.

Exportiere bis spätestens 08.01.2027 im Microsoft Purview-Portal unter Insider Risk Management › Alerts die Liste der verworfenen Alerts mit Gründen und Notizen, und lege sie revisionssicher und zugriffsbeschränkt ab. Wer später für eine Statistik oder ein Verfahren nachweisen muss, warum 2026 etwas verworfen wurde, wird dir danken.

Prüfe außerdem, ob Power-BI-Berichte, SIEM-Regeln oder Skripte das alte Grund-Feld auswerten. Die brechen still.

Wann	Wer	Was konkret
Bis 05.12.2026	IRM-Admin	Analysten und Ermittler informieren, wie es die Meldung empfiehlt. Rollengruppen prüfen: Wer klassifizieren darf, darf auch etikettieren.
Bis 18.12.2026	IRM-Admin, Ermittlungsleitung	Klassifizierungsleitfaden: Kriterien je Klasse, Begründungspflicht, Vier-Augen-Regel für True positive, Umgang mit Dubletten.
Bis 18.12.2026	IT-Leitung, DSB	Betriebs- oder Personalrat informieren, Anlage der Vereinbarung ergänzen, VVT und DSFA anpassen.
Dezember 2026	IRM-Admin	Preview beobachten: Erscheint die Spalte „Classification“ schon, Leitfaden an echten Alerts testen.
Bis 08.01.2027	IRM-Admin	Verworfene Alerts samt Dismiss-Gründen exportieren, Reports und Skripte inventarisieren.
Bis 15.01.2027	Ermittlungsleitung	Kurze Schulung: „Manage“ für den Status, „Classify“ für das Ergebnis, immer beides.
Bis 29.03.2027	IRM-Admin, Gremium	Erste Auswertung der Klassifizierung je Richtlinie, Schwellen nachjustieren, Ergebnis aggregiert berichten.

Warnung: „Manage“ ist kein Mülleimer

Die neue Oberfläche lädt dazu ein, Alerts im Akkord über „Manage“ zu verwerfen, ohne je „Classify“ zu öffnen. Genau so entsteht ein Datenfriedhof, in dem nach einem Jahr 3.000 unklassifizierte Leichen liegen und kein Mensch mehr sagen kann, ob die Richtlinie etwas taugt. Mach das Klassifizieren zur Pflicht vor dem Abschluss und prüf die Quote monatlich. Wer nicht klassifiziert, hat nicht ermittelt, sondern nur aufgeräumt.

Kommunikation an die Belegschaft: Eine Rundmail „Wir klassifizieren jetzt Insider-Risiken“ ist das kommunikative Äquivalent zu „Wir müssen reden“. Lass sie. Informiere über die bestehenden Kanäle zur IRM-Vereinbarung, sachlich: Alerts werden künftig mit einer begründeten Einordnung versehen, die meisten davon lauten erfahrungsgemäß „harmlos“ oder „Fehlalarm“, und Auswertungen erfolgen nur aggregiert. Dieser letzte Halbsatz ist der wichtigste, und er sollte stimmen.

Die Abläufe rund um Alerts, Status und Fälle beschreibt Microsoft im Learn-Artikel Untersuchen von Insider-Risikomanagement-Aktivitäten. Den Stand des Rollouts verfolgst du im Microsoft 365 Roadmap-Eintrag 576710.

Weiterlesen auf boddenberg.de

› Purview: DSGVO-Compliance-Tools
› Microsoft Purview als NIS2-Governance-Layer
› Defender, Entra und Purview erhalten neue Kontrollen für Agentic-AI-Sicherheit

Häufig gestellte Fragen

Ab wann gibt es in Purview Insider Risk Management keine Dismiss-Gründe mehr?

Laut Microsoft-Ankündigung MC1568697 wird die Alert-Klassifizierung ab Mitte Januar 2027 weltweit ausgerollt, der Rollout soll Ende Januar 2027 abgeschlossen sein. Mit der Klassifizierung ersetzt Microsoft die bisherigen Dismiss-Gründe; eine Public Preview läuft bereits ab Anfang Dezember 2026.

Was ist der Unterschied zwischen True positive, Benign positive und False positive in Insider Risk Management?

True positive bedeutet, dass die Aktivität stattfand und ein relevantes Geschäftsrisiko darstellt. Benign positive heißt, dass die Aktivität stattfand, aber erlaubt oder für die Rolle üblich war, und False positive, dass der Alert die Aktivität oder das Risiko nicht korrekt abbildet, etwa bei Dubletten oder automatisierten Prozessen.

Ändert sich der Status eines Insider-Risk-Alerts, wenn ich ihn klassifiziere?

Nein, Status und Klassifizierung sind unabhängig voneinander. Die Statusaktionen wie Bestätigen oder Verwerfen liegen künftig unter „Manage“, die Einordnung unter „Classify“, und keine der beiden Aktionen überschreibt die andere.

Muss der Betriebsrat der Alert-Klassifizierung in Insider Risk Management zustimmen?

Insider Risk Management ist eine technische Einrichtung zur Verhaltens- und Leistungskontrolle im Sinne von § 87 Abs. 1 Nr. 6 BetrVG, im öffentlichen Dienst gilt das Personalvertretungsrecht. Da die Klassifizierung eine neue Bewertung von Beschäftigten und neue Auswertungen ermöglicht, sollte sie vor dem Rollout in der bestehenden Vereinbarung geregelt oder vom Gremium ausdrücklich freigegeben sein.

Brauche ich für die neue Alert-Klassifizierung eine zusätzliche Lizenz?

Nein, die Klassifizierung ist Teil von Insider Risk Management und kostet nichts extra. Voraussetzung ist eine IRM-Lizenz, etwa über Microsoft 365 E5, A5 oder G5, E5 Compliance oder ein entsprechendes Add-on.