Prof. Dr. Andreas Igl
TH Deggendorf

Insider-Risiko nach DORA für Banken und andere Finanzunternehmen

Deggendorfer Notiz 2026/01 | 27. Januar 2026

Die europäische DORA-Verordnung rückt die digitale Resilienz von Banken in den Mittelpunkt regulatorischer Erwartungen. Während externe Cyberbedrohungen intensiv diskutiert werden, bleibt ein besonders sensibles Risiko häufig im Hintergrund: **der Insider**. Mitarbeitende, Dienstleister oder Partner verfügen über legitime Zugänge, tiefes Prozesswissen und gewachsene Vertrauensbeziehungen. Diese Notiz beleuchtet, warum Insider-Risiken strategisch gesteuert werden müssen und wie ein ganzheitlicher Ansatz unter DORA gestaltet werden kann.

1. Insider-Risiko im Finanzsektor: Einordnung und aktuelle Entwicklungen

Mit der zunehmenden Konkretisierung der europäischen Verordnung über digitale operationale Resilienz im Finanzsektor (DORA) rückt das IKT-Risikomanagement von Banken stärker in den Mittelpunkt regulatorischer Erwartungen. Während in der frühen Auseinandersetzung mit DORA vor allem externe Cyberbedrohungen und Drittparteirisiken diskutiert wurden, gewinnt ein besonders sensibles und häufig unterschätztes Themenfeld zunehmend an Bedeutung: das Insider-Risiko. Dieses Risiko ist keineswegs neu, erhält jedoch durch Digitalisierung, Cloud-Nutzung und neue Arbeitsmodelle eine neue Qualität und Dringlichkeit.

Im Unterschied zu externen Angreifern verfügt der Insider über einen entscheidenden strukturellen Vorteil. Er befindet sich bereits innerhalb der Organisation, besitzt legitime Zugriffsrechte und kennt Prozesse, Kontrollen und typische Erkennungsmuster. In vielen Fällen wurden über Jahre hinweg Informationen gesammelt, Beziehungen aufgebaut und interne Abläufe verinnerlicht. Dadurch entsteht ein Wissensvorsprung, der externe Angriffe erheblich erleichtern kann oder eigenständige schädliche Handlungen begünstigt. Besonders kritisch ist die Rolle des Menschen als soziales Wesen im organisationalen Kontext. Kollegialität, Vertrauen und gewachsene Zusammenarbeit bilden wichtige Grundlagen erfolgreicher Unternehmenskultur, können jedoch gleichzeitig dazu führen, dass Auffälligkeiten spät erkannt oder nicht konsequent adressiert werden.

Parallel dazu beobachten Sicherheitsbehörden eine zunehmende Professionalisierung externer Angreifer, die gezielt nach internen Zugangsmöglichkeiten suchen. Persönliche

Selbstdarstellung in sozialen Medien, etwa durch Hinweise auf neue Positionen mit administrativen Rechten, kann ungewollt als Einladung zur Kontaktaufnahme dienen. Treffen solche Gelegenheiten auf persönliche Belastungssituationen wie finanzielle Schwierigkeiten, gesundheitliche Probleme oder familiäre Konflikte, entsteht eine besonders kritische Gemengelage. Angreifer erkennen und nutzen diese Konstellationen systematisch.

Für Leitungsorgane ergibt sich daraus ein komplexes Spannungsfeld. Einerseits besteht die Pflicht, Risiken frühzeitig zu erkennen und entschlossen zu handeln. Andererseits besteht die berechtigte Sorge, dass ein Generalverdacht gegenüber Mitarbeitenden Motivation, Vertrauen und Unternehmenskultur nachhaltig beeinträchtigen könnte. Hinzu kommen arbeitsrechtliche Fragestellungen, die im Verdachtsfall schnelles und gleichzeitig rechtssicheres Handeln erfordern. Eine vorschnelle Freistellung kann langfristige Vertrauensbeziehungen irreparabel beschädigen, während zögerliches Handeln erhebliche Schäden nach sich ziehen kann. Die zentrale Herausforderung besteht daher darin, ein strukturiertes und verhältnismäßiges Vorgehen zu etablieren, das Prävention, Früherkennung und Reaktion in Einklang bringt.

2. Ganzheitliches Vorgehensmodell zur Steuerung von Insider-Bedrohungen

2.1 Klares Bedrohungsbild definieren

Ein belastbares Insider-Risikomanagement setzt zwingend bei einer präzisen Definition des Bedrohungsbildes an. In vielen Organisationen wird das Insider-Risiko entweder pauschal als Sonderfall des Cyber-Risikos betrachtet oder ausschließlich mit böswilligem Verhalten gleichgesetzt. Diese Verkürzung greift zu kurz und führt in der Praxis zu unzureichenden oder fehlgeleiteten Maßnahmen. Tatsächlich ist das Insider-Risiko ein vielschichtiges Phänomen, das technische, organisatorische und menschliche Faktoren miteinander verbindet und sich dynamisch über die Zeit verändert.

Eine differenzierte Insider-Typologie bildet den methodischen Ausgangspunkt. Böswillige Insider handeln vorsätzlich mit dem Ziel der Schädigung, etwa durch den Verkauf von Daten, gezielte Manipulation von Systemen oder Sabotage. Fahrlässige Insider hingegen verursachen Schäden unbeabsichtigt, beispielsweise durch Umgehung von Sicherheitsvorgaben, mangelnde Aufmerksamkeit oder unzureichendes Sicherheitsbewusstsein. Opportunistische Insider nutzen sich bietende Gelegenheiten, etwa bei unzureichender Kontrolle oder übermäßigen Berechtigungen, ohne langfristige Planung. Eine weitere besonders kritische Kategorie stellen erpresste Insider dar, die unter finanziellem, persönlichem oder ideologischem Druck von externen Akteuren zu Handlungen gedrängt werden.

Auf Basis dieser Typologie wird ein Use-Case-Katalog entwickelt, der konkrete Szenarien beschreibt. Dazu zählen etwa der Abfluss von Kundendaten, Marktmanipulationen im

Handelsumfeld, missbräuchliche Kreditentscheidungen, Social-Engineering-Fehler oder fortbestehende Systemzugriffe nach Kündigungen oder Rollenwechseln. Diese Szenarien werden systematisch bewertet, indem potenzielle Schadensdimensionen erfasst werden. Neben unmittelbaren finanziellen Schäden sind regulatorische Konsequenzen, operative Beeinträchtigungen und langfristige Reputationsschäden zu berücksichtigen.

Die Analyse erfolgt entlang der bankfachlichen Wertschöpfungskette. Kreditprozesse, Zahlungsverkehr, Handel, IT-Betrieb, HR-Funktionen und ausgelagerte Dienstleistungen weisen jeweils spezifische Insider-Risikoprofile auf. Ergänzend werden strukturelle Risikotreiber identifiziert, darunter Remote Work, Cloud-Architekturen, Outsourcing, Fachkräftemangel sowie zunehmende Arbeitsverdichtung. Eine explizite Lifecycle-Perspektive stellt sicher, dass Risiken beim Eintritt, während der Beschäftigung, bei Rollenwechseln und beim Austritt gleichermaßen betrachtet werden. Abschließend werden Risikoakzeptanz und Risikotoleranz definiert, um klare Leitplanken für Prävention und Reaktion festzulegen.

2.2 Kritische Rollen und Zugänge priorisieren

Nach der Definition des Bedrohungsbildes folgt die systematische Priorisierung kritischer Rollen, Funktionen und Zugänge. Banken verfügen über hochkomplexe Organisations- und IT-Strukturen, in denen zahlreiche Mitarbeitende legitime Zugriffsrechte auf sensible Systeme und Daten besitzen. Ohne klare Priorisierung entsteht schnell ein unüberschaubares Risikobild, das weder steuerbar noch wirksam adressierbar ist.

Im Zentrum steht die Identifikation von Schlüsselpositionen mit erhöhtem Missbrauchspotenzial. Dazu zählen insbesondere Rollen mit administrativen Systemrechten, hohem Transaktionsvolumen oder unmittelbarem Einfluss auf geschäftskritische Entscheidungen. IT-Administratoren, Mitarbeitende im Zahlungsverkehr, im Handel, in der Kreditvergabe sowie im Personalbereich sind hierbei regelmäßig besonders relevant. Ein strukturiertes Kritikalitätsmodell bewertet diese Rollen anhand klar definierter Kriterien wie Umfang der Datenzugriffe, Systemprivilegien, Möglichkeit zur Umgehung von Kontrollen und potenzieller Schadenshöhe.

Besondere Aufmerksamkeit gilt den sogenannten Crown Jewels der Bank. Hierzu zählen Zahlungsverkehrssysteme, zentrale Kundendatenbanken, Handelsplattformen, Risikomodelle und proprietäre Algorithmen. Für diese Systeme wird detailliert erfasst, welche Personen oder Funktionen Zugriff besitzen. Privilegierte Konten, Service-Accounts, Notfallzugänge und API-Schnittstellen werden vollständig inventarisiert, da gerade diese Zugänge häufig unzureichend überwacht werden.

Ein wesentlicher Aspekt ist die Einbindung externer Dienstleister. IT-Dienstleister, Berater, Entwickler oder Callcenter-Mitarbeitende verfügen oftmals über weitreichende Zugriffsrechte, ohne vollständig in interne Kontrollmechanismen eingebunden zu sein.

Rollenwechsel innerhalb der Organisation stellen zusätzliche Risikomomente dar, da Berechtigungen erweitert, jedoch nicht immer konsequent zurückgenommen werden. Der Joiner-Mover-Leaver-Prozess wird daher ganzheitlich analysiert. Kritische Kombinationen von Rollen und Rechten werden identifiziert und in Schutzbedarfsstufen überführt, die als Grundlage für priorisierte technische und organisatorische Maßnahmen dienen.

2.3 Need-to-know und Vier-Augen-Prinzip konsequent durchziehen

Ein zentrales Element der Insider-Risikoprävention ist die konsequente Umsetzung des Need-to-know-Prinzips. In der Praxis zeigt sich jedoch häufig eine schleichende Ausweitung von Berechtigungen über Jahre hinweg, die kaum noch hinterfragt wird. Historisch gewachsene Zugriffsrechte, projektbezogene Sonderfreigaben oder mangelnde Transparenz führen zu einem erheblichen Risiko.

Ein verbindliches Zielbild für Least Privilege definiert daher den Rahmen. Jede Rolle erhält ausschließlich die Rechte, die für die jeweilige Aufgabe zwingend erforderlich sind. Individuelle Berechtigungen werden weitgehend vermieden und durch standardisierte Rollenmodelle ersetzt. Parallel dazu wird die funktionale Trennung kritischer Tätigkeiten systematisch umgesetzt, um missbrauchsanfällige Kombinationen zu verhindern. Das Vier-Augen-Prinzip wird nicht nur formal festgeschrieben, sondern technisch und organisatorisch durchgesetzt.

Privilegierte Zugriffe werden über ein strukturiertes Privileged Access Management gesteuert. Administrative Rechte werden zeitlich begrenzt vergeben und vollständig protokolliert. Genehmigungsprozesse sind nachvollziehbar und revisionssicher dokumentiert. Notfallzugänge, sogenannte Break-Glass-Konten, unterliegen besonders strengen Kontrollen und werden regelmäßig überprüft.

Ein weiterer wesentlicher Baustein sind regelmäßige Rezertifizierungen. Führungskräfte bestätigen in festgelegten Intervallen die Berechtigungen ihrer Mitarbeitenden. Technische Unterstützung durch Identity-Governance-Lösungen automatisiert diesen Prozess und reduziert manuelle Fehler. Ergänzend werden Kennzahlen zur Berechtigungsreife etabliert, etwa der Anteil verwaister Konten oder privilegierter Nutzer. Dadurch entsteht Transparenz und eine belastbare Grundlage für kontinuierliche Verbesserung.

2.4 Früherkennung durch Monitoring und Anomalien

Da sich nicht jedes Insider-Risiko präventiv ausschließen lässt, kommt der Früherkennung eine zentrale Bedeutung zu. Ziel ist es, potenziell schädliche Aktivitäten möglichst frühzeitig zu erkennen, bevor es zu gravierenden Schäden kommt. Dabei ist ein ausgewogenes Verhältnis zwischen Sicherheit, Datenschutz und Unternehmenskultur erforderlich.

Ausgangspunkt ist die Definition einer Überwachungsstrategie. Es wird festgelegt, welche Aktivitäten überwacht werden dürfen und sollen. Baselines für normales Verhalten bilden die Grundlage für die Anomalieerkennung. Typische Arbeitszeiten, Zugriffsmuster, Transaktionsvolumina und Datenbewegungen werden analysiert, um Abweichungen sichtbar zu machen.

Risikobasierte Use-Cases adressieren typische Insider-Szenarien wie Massen-Downloads, ungewöhnliche Zugriffe auf sensible Daten, Umgehung von Sicherheitskontrollen oder Aktivitäten außerhalb üblicher Arbeitszeiten. Datenabfluss wird durch die Überwachung von Uploads, externen Speichern, Druckaktivitäten und E-Mail-Verkehr adressiert. Die Kombination mehrerer schwacher Signale erhöht die Aussagekraft und reduziert Fehlalarme.

Ein klar definiertes Alarmierungs- und Priorisierungskonzept stellt sicher, dass Hinweise angemessen bewertet und bearbeitet werden. Die Umsetzung erfolgt DSGVO-konform, transparent und unter Einbindung von Arbeitnehmervertretungen. Erkenntnisse aus realen Vorfällen fließen systematisch in die Weiterentwicklung der Use-Cases ein und erhöhen kontinuierlich die Wirksamkeit der Früherkennung.

2.5 Klare Eskalations- und Entscheidungswege im Ernstfall

Im Insider-Fall entscheidet Geschwindigkeit über Schadensausmaß und regulatorische Konsequenzen. Unklare Zuständigkeiten oder zögerliche Entscheidungen führen häufig zu Eskalationen, die vermeidbar gewesen wären. Daher werden Eskalations- und Entscheidungswege vorab verbindlich definiert.

Zunächst wird klar festgelegt, ab wann ein Verdacht als Insider-Incident gilt. Rollen und Verantwortlichkeiten von Vorstand, Compliance, HR, Recht, IT-Security und Kommunikation werden eindeutig beschrieben. Entscheidungsbefugnisse und Eskalationsschwellen sind transparent dokumentiert.

Beweis- und Dokumentationsprozesse stellen sicher, dass forensische Erkenntnisse rechtssicher erhoben und gespeichert werden. Parallel dazu werden arbeitsrechtliche Maßnahmen vorbereitet, etwa Zugriffsentzug, Freistellung oder Anhörung. Regulatorische Meldepflichten gegenüber Aufsichts- und Datenschutzbehörden werden im Vorfeld geklärt.

Zeitkritische Leitplanken definieren, welche Maßnahmen innerhalb der ersten 24 oder 72 Stunden zu erfolgen haben. Externe Partner wie Forensik-Dienstleister, spezialisierte Kanzleien und Kommunikationsberater werden in die Planung einbezogen. Klare Kriterien regeln die Einbindung des Vorstands und sichern eine angemessene Steuerung auf höchster Ebene.

2.6 Krisen- und Kommunikationsszenarien üben

Theoretische Konzepte entfalten ihre Wirkung erst, wenn sie im Ernstfall beherrscht werden. Regelmäßige Übungen sind daher ein unverzichtbarer Bestandteil eines wirksamen Insider-Risikomanagements. Ziel ist es, Ruhe, Geschwindigkeit und Konsistenz im Krisenfall sicherzustellen.

Realistische Szenarien werden entwickelt, etwa Datenabfluss, Handelsmanipulation oder Sabotage. In Tabletop-Exercises werden Entscheidungsprozesse, Eskalationswege und Kommunikationsabläufe getestet. Führungskräfte und relevante Funktionen nehmen regelmäßig teil, um Handlungssicherheit zu gewinnen.

Ein besonderer Fokus liegt auf der Kommunikation. Externe Stakeholder wie Kunden, Aufsicht und Öffentlichkeit erfordern abgestimmte Botschaften. Sprecherrollen werden klar definiert. Interne Kommunikation stellt sicher, dass Mitarbeitende informiert werden, ohne Unsicherheit oder Panik zu erzeugen. Kommunikationsleitlinien balancieren Transparenz und Ermittlungsinteressen.

Krisenhandbücher mit vorbereiteten Abläufen, Checklisten und Statements unterstützen die schnelle Reaktion. Erkenntnisse aus Übungen werden systematisch ausgewertet und in Prozesse, Schulungen und technische Maßnahmen zurückgeführt.

2.7 Kultur und Anreizsysteme ernst nehmen

Langfristig wirksames Insider-Risikomanagement ist ohne eine tragfähige Unternehmenskultur nicht möglich. Technische Kontrollen allein können menschliche Faktoren nicht kompensieren. Eine offene Speak-up-Kultur fördert die frühzeitige Meldung von Auffälligkeiten und reduziert die Wahrscheinlichkeit eskalierender Vorfälle.

Psychologische Sicherheit ermöglicht es Mitarbeitenden, Bedenken ohne Angst vor Repression zu äußern. Sichere und unabhängige Whistleblower-Kanäle unterstützen diesen Ansatz. Führungskräfte werden sensibilisiert, Verhaltensänderungen und Warnsignale zu erkennen. Insider-Risiken werden als Bestandteil der Sicherheitskultur in Onboarding und Weiterbildung verankert.

Ethik- und Verhaltenskodizes definieren klare Erwartungen an Integrität und Verantwortungsbewusstsein. Belastungs- und Stressfaktoren werden als Risikotreiber ernst genommen. Anreiz- und Bonussysteme werden überprüft, um ungewollte Fehlanreize zu vermeiden. Vertrauensvolle HR-Prozesse unterstützen Mitarbeitende bei persönlichen oder beruflichen Problemen und tragen damit aktiv zur Risikoreduktion bei.

3. Leitlinien und Ressourcen deutscher Behörden zum Insider-Risiko

Die Auseinandersetzung mit Insider-Risiken wird in Deutschland maßgeblich durch Bundesbehörden und Sicherheitsinstitutionen geprägt. Für Banken sind insbesondere Veröffentlichungen des Bundesamts für Sicherheit in der Informationstechnik, des Bundesamts für Verfassungsschutz sowie der Polizeibehörden relevant.

Das Bundesamt für Sicherheit in der Informationstechnik stellt eine zentrale Referenzquelle dar. Der jährliche Lagebericht zur IT-Sicherheit beschreibt die Bedrohungslage weiterhin als besorgniserregend und betont die Rolle von Mitarbeitenden als Teil der Angriffsfläche. IT-Grundschutz und BSI-Standard 200-3 bieten einen etablierten Rahmen für Risikomanagement und Informationssicherheitsmanagement. Ergänzend stellen Threat-Intelligence-Analysen und Leitfäden zur Incident-Response praxisnahe Unterstützung bereit.

Das Bundesamt für Verfassungsschutz adressiert Insider-Risiken insbesondere im Kontext von Wirtschaftsspionage und Sabotage. Publikationen zum Wirtschaftsschutz betonen die Notwendigkeit ganzheitlicher Sicherheitskonzepte und weisen auf Radikalisierung, Erpressung und Anwerbung durch fremde Nachrichtendienste hin. Für Banken ergibt sich daraus eine besondere Verantwortung zum Schutz sensibler Finanz- und Kundendaten sowie kritischer Infrastruktur.

Das Bundeskriminalamt liefert die kriminalpolizeiliche Perspektive auf Cybercrime. Nationale Lagebilder zeigen steigende Angriffszahlen und die wachsende Bedeutung von Zugangsdatenhandel. Insider werden zunehmend als Bestandteil komplexer Angriffsketten betrachtet. Die Zusammenarbeit zwischen BKA, BSI und Landesbehörden unterstützt Ermittlungen und Prävention.

Landeskriminalämter und Zentrale Ansprechpartner Cybercrime fungieren als unmittelbare Ansprechpartner für Unternehmen. Sie bieten Beratung, unterstützen bei Forensik und fördern Präventionspartnerschaften. Für Banken stellen diese Strukturen wichtige Anlaufstellen im Ernstfall dar und ergänzen die eigene Sicherheitsarchitektur.

Prof. Dr. Andreas Igl
BDO-Stiftungsprofessor an der TH Deggendorf
Lehrbeauftragter an der Hochschule der Deutschen Bundesbank

andreas.igl@th-deg.de
(Mobil): 0151 2301 8610
(LinkedIn): Link