ISB-Modelle im Vergleich

EXTERN VS INTERN

BlackMount

ISB-Modelle im Vergleich

INHALT

ISB: extern vs intern

Warum dieser Leitfaden?

Einen Informationssicherheitsbeauftragten (ISB) zu benennen ist schnell erledigt. Einen wirksamen zu haben, deutlich seltener. In vielen Unternehmen ist der ISB eine formale Rolle – vergeben aus Pflichtgefühl, Zeitmangel oder nach dem Prinzip „Das macht jemand mit“.

Das Problem: Informationssicherheit scheitert nicht an Technik, sondern an falschen Entscheidungen. Der ISB wird oft als organisatorische Pflicht verstanden, nicht als Rolle mit echter Wirkung, Verantwortung und Einfluss. Genau hier entstehen Unsicherheit, Überforderung und im Ernstfall teure Fehlentscheidungen.

Dieser Leitfaden richtet sich an Entscheider, die keine Alibi-Lösung wollen, sondern verstehen möchten, warum die Besetzung der ISB-Rolle über Risiko, Haftung und Belastbarkeit der Organisation entscheidet und warum „intern“ dabei oft die bequemste, aber riskanteste Wahl ist.

Jannik Christ
Geschäftsführer
CISSP | CCSP | CISM | ISO/IEC 27001 Lead Auditor / Lead Implementer
§8a Prüfverfahrenskompetenz (KRITIS)

Was ein ISB wirklich leisten muss

Der Informationssicherheitsbeauftragte ist keine Dokumentationsstelle und kein verlängerter Arm der IT. Wer glaubt, der ISB bestehe aus Richtlinienpflege, Maßnahmenlisten und Auditbegleitung, verwechselt Beschäftigung mit Wirkung.

Die eigentliche Aufgabe eines ISB ist unbequemer: Er muss Risiken sichtbar machen, Entscheidungen erzwingen und Widersprüche offenlegen. Nicht technisch, sondern organisatorisch. Nicht theoretisch, sondern im konkreten Unternehmenskontext. Informationssicherheit scheitert selten an fehlenden Maßnahmen – sie scheitert daran, dass niemand klar benennt, was notwendig ist, was übertrieben ist und was bewusst akzeptiert wird.

Ein wirksamer ISB bewertet Risiken nicht aus dem Bauch heraus, sondern strukturiert und nachvollziehbar. Er priorisiert, wo andere alles gleichzeitig lösen wollen. Er sagt auch „Nein“, wenn Maßnahmen zwar gut klingen, aber keinen echten Sicherheitsgewinn bringen. Genau das macht ihn unbequem – und genau das macht ihn wertvoll.

Zu den Kernaufgaben eines ISB gehört es außerdem, Informationssicherheit erklärbar zu machen. Nicht in Fachbegriffen, sondern in Auswirkungen: auf Geschäftsprozesse, Haftung, Verfügbarkeit und Reputation. Wenn die Geschäftsführung nach einem Gespräch mit dem ISB nicht klar sagen kann, wo die größten Risiken liegen und warum, hat der ISB seine Aufgabe verfehlt.

In der Praxis wird diese Rolle jedoch häufig Personen übertragen, die weder Zeit noch Rückendeckung haben. Der ISB soll Risiken bewerten, darf aber niemandem widersprechen. Er soll Anforderungen umsetzen, ohne Prioritäten setzen zu dürfen. Er soll Sicherheit herstellen, ohne Einfluss auf Entscheidungen zu haben. Das Ergebnis ist vorhersehbar: viel Aktivität, wenig Wirkung.

Ein guter ISB ist nicht derjenige, der alles absichert. Er ist derjenige, der Transparenz schafft, Verantwortung einfordert und Informationssicherheit aus der Komfortzone holt. Wer einen ISB sucht, der vor allem „mitläuft“, bekommt genau das, was er bestellt hat: eine Rolle ohne Relevanz und Sicherheit ohne Substanz.

Die häufigsten Fehler bei der ISB-Besetzung

Fehlbesetzungen beim ISB passieren selten aus böser Absicht. Sie entstehen aus Pragmatismus, Zeitdruck und dem Wunsch, ein Thema möglichst schnell „erledigt“ zu haben. Das Problem: Informationssicherheit verzeiht diese Abkürzungen nicht.

Im Folgenden finden Sie die häufigsten ISB-Fehlbesetzungen aus der Praxis. Wenn Sie sich hier wiederfinden, ist das kein Vorwurf, aber ein klares Warnsignal.

“Das macht jemand aus der IT mit”

Der Klassiker. Der ISB wird dort angesiedelt, wo man ihn vermutet: in der IT. Zusätzlich zum Tagesgeschäft, ohne klare Priorität und ohne echte Trennung zwischen Betrieb und Kontrolle.

Das Problem dahinter: Der ISB soll Risiken bewerten, die oft direkt aus der eigenen IT stammen. Objektivität sieht anders aus. Was entsteht, ist kein unabhängiger Blick, sondern eine Mischung aus Betriebsblindheit, Rechtfertigung und Konfliktvermeidung. Wer den ISB in der IT „mitlaufen lässt“, bekommt Sicherheitsgefühl statt Sicherheit.

“Der ISB ist bei uns eher formell”

Hier ist der ISB benannt, aber nicht ernsthaft eingebunden. Die Rolle existiert auf dem Organigramm, nicht im Entscheidungsprozess. Risiken werden dokumentiert, aber nicht diskutiert. Maßnahmen werden beschrieben, aber nicht priorisiert.

Ein formeller ISB ist kein Sicherheitsgewinn, sondern ein Scheinschutz.

Er beruhigt intern – und bricht extern sofort zusammen, sobald kritische Fragen gestellt werden.

“Für das Audit wird es reichen”

In diesem Szenario wird der ISB ausschließlich durch die Brille der nächsten Prüfung betrachtet. Hauptziel: bestehen. Alles andere ist nachrangig.

Ein ISB, der nur auf Audits ausgerichtet ist, optimiert für den Stichtag, nicht für den Ernstfall. Sobald Anforderungen steigen oder sich Rahmenbedingungen ändern, fehlt jede Substanz. Wenn es dann doch zu einem Ernstfall kommt, fällt das System in sich zusammen.

Die häufigsten Fehler bei der ISB-Besetzung

“Der ISB soll bitte niemandem wehtun”

Es wird bewusst jemand gewählt, der angepasst ist. Konfliktscheu. „Vermittelnd“. Risiken werden weich formuliert, Prioritäten vorsichtig relativiert, kritische Themen hinausgeschoben.

Informationssicherheit ohne Reibung ist wirkungslos. Ein ISB, der niemanden irritiert, schützt auch niemanden. Sicherheit entsteht nicht durch Harmonie, sondern durch Klarheit.

Ein ISB, der nicht unbequem sein darf, ist strukturell handlungsunfähig.

“Der ISB bekommt kein echtes Mandat”

Vielleicht die gefährlichste Fehlbesetzung: Der ISB soll liefern, aber nichts entscheiden. Er soll Risiken benennen, aber nichts einfordern. Er trägt Verantwortung, aber keine Autorität.

Ohne Mandat wird der ISB zum Bittsteller. Entscheidungen werden verschoben, Maßnahmen verwässert, Risiken akzeptiert – ohne dass jemand bewusst dazu steht.

Das Ergebnis ist kein Sicherheitskonzept, sondern organisierte Verantwortungs-losigkeit.

Interne oder externe Besetzung?

Die Frage, ob der Informationssicherheitsbeauftragte intern oder extern besetzt wird, wird in vielen Unternehmen erstaunlich kurz diskutiert. „Intern ist näher dran“, „Intern ist günstiger“, „Intern kennen wir die Person.“
Das klingt vernünftig, ist aber oft genau der Denkfehler, der später teuer wird.

Ein interner ISB ist Teil der Organisation. Er ist eingebunden in Hierarchien, Abhängigkeiten und bestehende Entscheidungen. Genau dort liegt das Problem. Der ISB soll Risiken bewerten, die häufig aus den eigenen Strukturen entstehen. Er soll Entscheidungen hinterfragen, an denen er selbst beteiligt war. Objektivität wird so zur Wunschvorstellung.

Hinzu kommt: Ein interner ISB arbeitet fast nie ausschließlich als ISB. Die Rolle wird „mitgemacht“, zwischen Tagesgeschäft, Projektarbeit und operativem Druck. Zeit für Einordnung, Priorisierung und saubere Steuerung bleibt selten. Das Ergebnis ist bekannt: viel Aktivität, wenig Wirkung und eine Sicherheitsorganisation, die vor allem intern beruhigt.

Der externe ISB startet aus einer anderen Position. Er bringt Distanz mit und genau diese Distanz ist seine Stärke. Er bewertet Risiken ohne Rücksicht auf interne Befindlichkeiten, benennt Zielkonflikte klar und kann unangenehme Fragen stellen, ohne sich selbst zu schützen. Nicht, weil er es besser weiß, sondern weil er es darf.

Externe ISBs sind zudem nicht auf Einzelfälle beschränkt. Sie bringen jede Menge Erfahrungen aus den unterschiedlichsten Branchen mit und sehen Muster. Sie wissen, welche Lösungen funktionieren und welche regelmäßig scheitern. Sie erkennen früh, wo Maßnahmen überdimensioniert sind und wo echte Lücken bestehen. Diese Erfahrung lässt sich intern kaum aufbauen, ohne jahrelang Fehler zu machen.

Oft wird argumentiert, ein externer ISB sei „weiter weg“. In der Praxis ist häufig das Gegenteil der Fall. Während interne ISBs zwischen Rollen und Erwartungen zerrieben werden, hat der externe ISB ein klares Mandat, klare Aufgaben und einen klaren Fokus. Nähe entsteht nicht durch Anwesenheit, sondern durch Wirksamkeit.

Der interne ISB fühlt sich vertraut an, der externe ISB wirkt. Wer sein Unternehmen schützen will und Informationssicherheit ernst nimmt, entscheidet sich nicht für die bequemste Lösung, sondern für die, die langfristig entlastet, Risiken reduziert und Klarheit schafft.

Die 7 entscheidenden Auswahlkriterien

Einen ISB zu benennen ist einfach. Einen geeigneten auszuwählen, deutlich schwerer. Viele Entscheidungen werden aus Gewohnheit, Nähe oder Bequemlichkeit getroffen – nicht anhand klarer Kriterien. Genau deshalb scheitert die ISB-Rolle in der Praxis so häufig.

Die folgenden Kriterien sind keine Wunschliste. Sie sind Mindestanforderungen. Wenn eines davon fehlt, ist der ISB keine Lösung, sondern ein Risiko.

1 Unabhängigkeit

Ein ISB, der eigene Entscheidungen, eigene Systeme oder eigene Abteilungen bewerten muss, ist nicht unabhängig. Punkt. Objektivität ist keine Charaktereigenschaft, sondern eine strukturelle Voraussetzung.

Wer den ISB intern verankert, muss sich bewusst sein: Nähe schafft Verständnis – aber sie zerstört Distanz. Ein ISB ohne echte Unabhängigkeit wird Risiken weichzeichnen, Konflikte vermeiden und Probleme verschieben.

2 Ein klares Mandat, nicht nur ein Titel

Ein Informationssicherheitsbeauftragter ohne klares Mandat ist von Beginn an wirkungslos. Wenn Risiken zwar erkannt, aber nicht eingefordert oder eskaliert werden dürfen, bleibt Sicherheit ein formaler Akt ohne Wirkung. Ein Titel ersetzt keine Entscheidungsbefugnis.

Ein wirksamer ISB muss gehört werden – auch wenn es unbequem wird. Fehlt die Rückendeckung des Managements, endet die Rolle bei der Dokumentation. Ein ISB ohne Mandat suggeriert Sicherheit, wo in Wirklichkeit niemand handeln darf.

3 Fähigkeit zur Priorisierung

Informationssicherheit scheitert nicht nur an zu wenigen Maßnahmen, sondern auch an zu vielen, ohne klare Reihenfolge. Ein ISB, der alles für kritisch erklärt, schafft keine Sicherheit, sondern Unruhe. Maßnahmen häufen sich, Entscheidungen werden vertagt und niemand weiß, was wirklich zählt.

Ein wirksamer ISB priorisiert konsequent. Er benennt die größten Risiken, stellt anderes bewusst zurück und kommuniziert diese Entscheidungen klar. Das ist unbequemer als alles „mitzunehmen“, aber genau darin liegt Wirkung. Ohne Priorisierung entsteht keine Sicherheit, nur dauerhafte Betriebsamkeit.

Die 7 entscheidenden Auswahlkriterien

4 Verständlichkeit

Ein ISB, den nur Fachleute verstehen, hat seinen Zweck verfehlt. Die wichtigste Zielgruppe des ISB ist nicht die IT, sondern die Unternehmensleitung.

Risiken müssen so erklärt werden, dass Entscheidungen möglich sind. Nicht so, dass Rückfragen entstehen.

5 Praxiserfahrung

Informationssicherheit lässt sich nicht aus Büchern oder Normenkapiteln heraus steuern. Ein ISB, der ausschließlich theoretisches Wissen mitbringt, erkennt Probleme oft erst, wenn sie bereits eskaliert sind. Normen beschreiben, wasgefordert ist – sie sagen aber nichts darüber, wie sich Anforderungen im realen Unternehmensalltag durchsetzen lassen.

Ein wirksamer ISB kennt die typischen Bruchstellen zwischen Anspruch und Realität. Er weiß, wo Maßnahmen scheitern, weil Ressourcen fehlen, Prioritäten kollidieren oder Organisationen überfordert sind. Diese Erfahrung lässt sich nicht simulieren. Wer Informationssicherheit wirksam gestalten will, braucht einen ISB, der Praxis erlebt hat – nicht nur Schulungen besucht.

6 Durchhaltevermögen

Informationssicherheit ist kein Projekt mit Enddatum, sondern eine dauerhafte Führungsaufgabe.

Ein ISB, der nur für Prüfungen sichtbar wird, verwaltet Anforderungen. Er steuert keine Sicherheit. Nach dem bestandenen Audit verschwindet das Thema wieder im Tagesgeschäft, bis der nächste externe Druck entsteht.

Ein wirksamer ISB bleibt präsent, auch wenn niemand danach fragt. Er sorgt dafür, dass Entscheidungen Bestand haben und IT-Sicherheit nicht zur saisonalen Aufgabe verkommt. Ohne Durchhaltevermögen bleibt IT-Sicherheit eine Momentaufnahme und genau darauf verlassen sich Angreifer.

7 Neutralität

Sobald Empfehlungen von internen Abhängigkeiten oder eigenen Interessen geprägt sind, verliert die Rolle ihre Glaubwürdigkeit. Sicherheit wird dann nicht nach Risiko, sondern nach Bequemlichkeit bewertet.

Ein ISB empfiehlt Maßnahmen, weil sie notwendig sind und nicht, weil sie intern passen oder sich besser verkaufen lassen. Ohne Neutralität wird Informationssicherheit zur Meinungsfrage.

Warum externe ISBs die Kriterien häufig erfüllen

Ein externer ISB hat einen entscheidenden Vorteil: Er schuldet niemandem Loyalität außer dem Auftrag. Er muss keine bestehenden Entscheidungen rechtfertigen, keine Abteilungen schonen und keine Karrierepfade berücksichtigen. Diese Distanz ist unbequem – und genau deshalb wirksam. Wo interne ISBs erklären, relativieren und vermitteln, darf der externe ISB klar benennen.

Auch das Mandat ist kein Zufall. Externe ISBs werden nicht „mitgemacht", sondern bewusst beauftragt. Mit klaren Erwartungen, klaren Aufgaben und direktem Zugang zum Management.

Erfahrung ist ein weiterer Punkt, der intern kaum aufzuholen ist. Externe ISBs sehen immer wieder dieselben Muster: überforderte Rollen, falsche Prioritäten, Sicherheitsmaßnahmen ohne Wirkung.

Sie wissen, was funktioniert und was regelmäßig scheitert. Interne ISBs lernen diese Lektionen meist erst, wenn es bereits teuer geworden ist. Auch Priorisierung fällt extern leichter. Wer nicht im Tagesgeschäft gefangen ist, kann Risiken nüchtern bewerten. Externe ISBs müssen niemandem gefallen. Sie müssen nicht integrieren, sie müssen steuern. Genau deshalb orientieren sich ihre Empfehlungen häufiger an Wirkung statt an Konsens.

Die unbequeme Wahrheit lautet daher:
Ein interner ISB kann sehr engagiert sein – und trotzdem wirkungslos bleiben. Nicht wegen mangelnder Kompetenz, sondern wegen struktureller Einschränkungen. Externe ISBs sind nicht automatisch besser. Aber sie arbeiten unter Bedingungen, die Informationssicherheit überhaupt erst möglich machen.

EXTERNER ISB	INTERNER ISB
✓ Erkennt Risiken, weil er sie schon gesehen hat	✗ Lernt Sicherheit am eigenen Unternehmen
✓ Sofort Einsatzbereit	✗ Monate Stillstand durch Recruiting und Einarbeitung
✓ IT-Sicherheit kennt keine Ausfallzeiten	✗ Ausfälle bei Krankheit, Urlaub etc.
✓ Kostengünstiger, da Zahlung sich nach Bedarf berechnet	✗ Teure Fixkosten, unabhängig vom Ergebnis
✓ Unabhängig & klar	✗ Gefahr der Betriebsblindheit & interne Abhängigkeiten
✓ Ziel:Angriffe verhindern	✗ Ziel: Audit bestehen

Das können Unternehmen von einem externen ISB konkret erwarten

Externer ISB ist nicht gleich externer ISB. Der Markt ist groß, unübersichtlich und teilweise trügerisch. Viele Unternehmen entscheiden sich bewusst gegen einen internen ISB, landen aber dennoch bei einer Lösung, die am Kern der Aufgabe vorbeigeht.

Es gibt externe Dienstleister, die im Wesentlichen ihren Namen zur Verfügung stellen. Sie erfüllen formale Anforderungen, bringen die notwendigen Qualifikationen mit und tauchen in Dokumenten, Richtlinien oder auf der Website als ISB auf. Auf dem Papier ist damit alles erledigt. In der Praxis ändert sich nichts.

Diese Modelle sind oft günstig. Und genau das ist ihr größter Reiz. Sie vermitteln Sicherheit, ohne sie zu erzeugen. Sie sorgen dafür, dass Anforderungen erfüllt scheinen, nicht dafür, dass Informationssicherheit im Unternehmen tatsächlich gelebt wird. Für das Sicherheitsniveau, die Entscheidungsfähigkeit und die Resilienz der Organisation haben sie kaum Wirkung.

Ein wirksamer externer ISB geht einen völlig anderen Weg. Er beschränkt sich nicht auf formale Präsenz, sondern übernimmt die Rolle aktiv. Er ist sichtbar, ansprechbar und eingebunden. Er kennt Prozesse, Schnittstellen und Entscheidungswege. Informationssicherheit wird dadurch Teil des Arbeitsalltags und nicht nur Teil der Dokumentation.

Unternehmen sollten von einem externen ISB erwarten, dass er nicht nur Anforderungen kennt, sondern Verantwortung übernimmt. Dass er nicht nur benennt, sondern begleitet. Dass er nicht nur qualifiziert ist, sondern präsent. IT-Sicherheit lässt sich nicht delegieren und schon gar nicht „outsourcen“, ohne sie zu leben. Genau hier trennt sich formale Erfüllung von wirksamer Sicherheitsarbeit.

Ein externer ISB, der Wirkung entfaltet, sorgt dafür, dass Informationssicherheit im Unternehmen verstanden, akzeptiert und umgesetzt wird. Er schafft Verbindlichkeit, statt nur Nachweise. Er unterstützt Entscheidungen, statt sie zu umgehen. Und er bleibt dran, statt sich auf formale Rollenbeschreibungen zurückzuziehen.

Die unbequeme Wahrheit lautet deshalb:
Ein günstiger externer ISB kann teuer werden. Und zwar nicht durch seine Rechnung, sondern durch das trügerische Gefühl von Sicherheit, das er erzeugt.

Unser Ansatz: Externer ISB bei BlackMount

Unser Anspruch ist nicht, als Dienstleister „hinzugezogen“ zu werden, sondern als fester Bestandteil der Organisation zu arbeiten. Ein externer ISB von BlackMount sitzt nicht am Rand, sondern mit am Tisch.

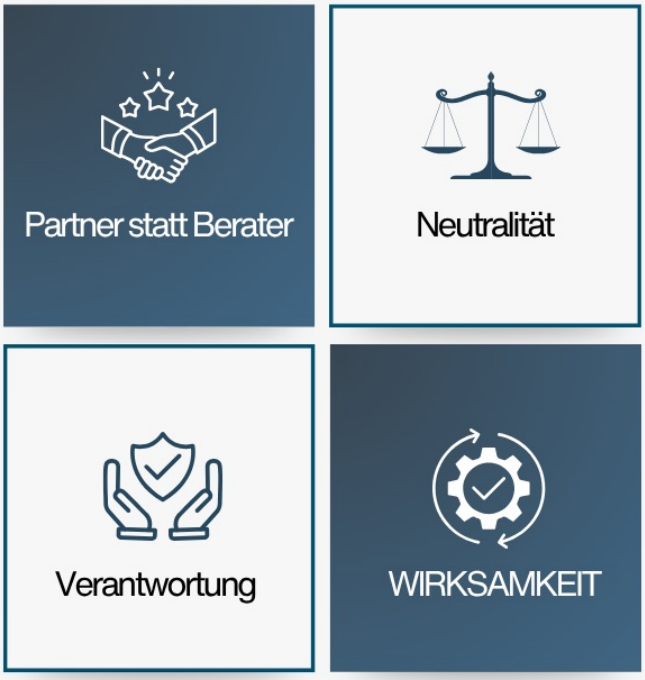
In der Zusammenarbeit mit unseren Kunden verschwimmt sehr schnell die Frage, ob der ISB intern oder extern ist. Nicht, weil Rollen unklar wären, sondern weil Integration konsequent gelebt wird. Wir sind tief in Prozesse, Entscheidungswege und Abläufe eingebunden. Wir kennen die Organisation, die Menschen und die realen Zwänge – nicht aus Präsentationen, sondern aus dem Arbeitsalltag.

Genau darin liegt unser Ansatz: Wir arbeiten nicht für das Unternehmen, sondern im Unternehmen. Wir denken mit, fragen nach, haken ein und bleiben dran. Informationssicherheit wird dadurch kein externes Thema, sondern Teil der täglichen Entscheidungsfindung. Der Unterschied ist spürbar. Vor allem dort, wo andere ISB-Modelle an der Oberfläche bleiben.

Gleichzeitig behalten wir bewusst das, was intern oft verloren geht: Distanz und Neutralität. Wir sind integriert, aber nicht verstrickt. Wir verstehen Abläufe, ohne sie zu verteidigen. Wir kennen Entscheidungen, ohne sie rechtfertigen zu müssen. Das erlaubt Klartext – auch dann, wenn es unbequem ist.

Für unsere Kunden bedeutet das: ein ISB, der jederzeit ansprechbar ist, Zusammenhänge kennt und Verantwortung übernimmt, ohne zusätzliche Reibung zu erzeugen. Kein Rollenwechsel, kein „externer Termin“, kein Übersetzen zwischen Welten. Es fühlt sich an, als würde BlackMount dazugehören – weil wir dazugehören.

Kurz gesagt:
Unser externer ISB ist kein Fremdkörper. Er ist Teil der Organisation – mit dem Vorteil, genau dort unabhängig zu bleiben, wo es für wirksame Informationssicherheit notwendig ist.



Fazit: Der richtige ISB

Der Informationssicherheitsbeauftragte ist keine formale Rolle und kein organisatorisches Pflichtfeld. Er ist eine bewusste Entscheidung darüber, wie ein Unternehmen mit Risiken, Verantwortung und Unsicherheit umgeht. Wer den ISB lediglich benennt, um Anforderungen zu erfüllen, investiert in Beruhigung – nicht in Sicherheit.

Die Praxis zeigt: Viele Probleme in der Informationssicherheit entstehen nicht durch fehlende Maßnahmen, sondern durch fehlende Klarheit. Unklare Zuständigkeiten, fehlende Priorisierung und mangelnde Unabhängigkeit führen dazu, dass Sicherheit zwar dokumentiert, aber nicht gelebt wird. Genau hier entscheidet sich, ob der ISB Wirkung entfaltet oder zur Formalie wird.

Ein externer ISB kann diese Lücke schließen – wenn die Rolle aktiv, integriert und konsequent ausgefüllt wird. Nicht jeder externe ISB tut das. Aber dort, wo Erfahrung, Neutralität, Präsenz und klare Mandate zusammenkommen, wird Informationssicherheit steuerbar, verständlich und dauerhaft wirksam.

Checkliste: Den richtigen ISB finden

Rolle & Mandat

- ☐ Ist die ISB-Rolle klar definiert?
- ☐ Hat der ISB direkten Zugang zur Geschäftsführung?
- ☐ Darf er Risiken klar benennen und eskalieren, auch wenn es unbequem ist?
- ☐ Ist geregelt, wo seine Verantwortung beginnt und endet?

Unabhängigkeit & Objektivität

- ☐ Bewertet der ISB Risiken ohne eigene Entscheidungen rechtfertigen zu müssen?
- ☐ Ist er frei von internen Abhängigkeiten oder wirtschaftlichen Interessen?
- ☐ Gibt es keine versteckte Tool- oder Produktbewerbung?
- ☐ Wird Neutralität gelebt und nicht nur behauptet?

Wirksamkeit statt Aktionismus

- ☐ Kann der ISB klar sagen, welche Risiken aktuell wirklich kritisch sind?
- ☐ Setzt er Prioritäten, statt alles gleichzeitig abzusichern?
- ☐ Kann er erklären und begründen, was bewusst nicht getan wird?
- ☐ Entstehen Entscheidungen oder nur Maßnahmenlisten?

Verständlichkeit & Management-Tauglichkeit

- ☐ Kann der ISB Risiken verständlich für Entscheider erklären?
- ☐ Weiß die Geschäftsführung nach Gesprächen, wo das Unternehmen steht?
- ☐ Fördert der ISB Entscheidungen statt neue Unsicherheit zu erzeugen?
- ☐ Wird Informationssicherheit als Führungsaufgabe vermittelt?

Erfahrung & Praxisnähe

- ☐ Hat der ISB nachweisbare Praxiserfahrung und nicht nur Zertifikate?
- ☐ Kennt er reale Audit-, Incident- und Umsetzungssituationen?
- ☐ Weiß er, was funktioniert und was regelmäßig scheitert?

Kontinuität & Verlässlichkeit

- ☐ Bleibt der ISB an Themen dran, auch wenn der Druck nachlässt?
- ☐ Ist die dauerhafte Verfügbarkeit gegeben?
- ☐ Ist die Rolle langfristig, nicht projektbezogen?

BlackMount

Turning Strategy into Security.

In einer Welt, in der Cyberrisiken zum Tagesgeschäft gehören und gesetzliche Anforderungen stetig steigen, reicht es nicht mehr aus, Informationssicherheit nur technisch zu betrachten.

Unser Antrieb ist es, Informationssicherheit ganzheitlich zu denken: als Zusammenspiel aus unternehmerischer Strategie, Prozessen, Menschen und Technologie. Wir sind davon überzeugt, dass Informationssicherheit dann besonders wirksam ist, wenn sie strategisch im Unternehmen verankert ist, zum Geschäftsmodell passt und nicht als notwendiges Übel betrachtet wird.

Was uns dabei antreibt? Unsere Leidenschaft für exzellente Beratung, unser Anspruch an nachhaltige Wirksamkeit und unser tiefes Verständnis für die realen Herausforderungen in Unternehmen.

Als Dankeschön für Ihr Interesse an unserem Whitepaper möchten wir Ihnen heute etwas Besonderes anbieten:

Ihr kostenloses Strategiegespräch:

Was Sie konkret nach dieser Stunde in den Händen halten

Status Quo: Eine objektive Einschätzung Ihrer derzeitigen Aufstellung und Identifikation kritischer Lücken.

Maßnahmenplan: Ein erster Fahrplan mit konkreten Schritten zur Umsetzung, abgestimmt auf Ihre individuellen Geschäftsprozesse und regulatorischen Anforderungen (wie z. B. NIS 2).

Entscheidungssicherheit: Die Gewissheit, ob eine interne Lösung für Sie tragfähig ist oder wie ein externer Partner Sie ohne bürokratischen Ballast absichern kann.

Termin buchen

Kontakt

info@blackmount.de

+49 (0) 800 / 5200 112

www.blackmount.de