NIS2, BCM und Audit: Warum viele Projekte feststecken

Endlich in die Umsetzung kommen

Strukturen, Anforderungen und Tools sind vielerorts vorhanden – dennoch stockt die operative Umsetzung. Es sind zumeist organisatorische Hürden die NIS2-, ISMS- und BCM-Initiativen ausbremsen. Unternehmen können mit klarer Governance, verbindlichen Verantwortlichkeiten und kontinuierlicher Steuerung echte Resilienz schaffen.

Viele Unternehmen haben die ersten Schritte in Richtung NIS2, ISM- oder BCM-Umsetzung bereits hinter sich. Strukturen wurden aufgebaut, Anforderungen analysiert und Software-Tools eingeführt. Und dennoch zeigt sich nach der Initialphase häufig das gleiche Bild: Die Grundlagen sind da – doch die operative Umsetzung kommt nicht voran.

Was in Konzepten schlüssig erscheint, erweist sich im Alltag oft als schwer steuerbar. Maßnahmen werden begonnen, aber nicht konsequent verfolgt. Verantwortlichkeiten sind zwar definiert, allerdings nicht wirksam verankert. Spätestens beim Audit entsteht wieder enormer manueller Aufwand. Die eigentliche Herausforderung beginnt also erst nach den ersten Projektschritten. Und so scheitert Compliance dann oft am »Silodenken« und fehlenden Personalkapazitäten, nicht an der extra eingekauften Software.

Wenn Umsetzung zur Dauerbaustelle wird: Die typischen Symptome.

In der Praxis zeigt sich bei vielen Organisationen ein ähnliches Muster. Anforderungen sind dokumentiert, Risiken bewertet. Dennoch fehlt es an Verbindlichkeit im operativen Alltag. Die vier häufigsten Symptome dafür sind:

- **Maßnahmen ohne Steuerung**
  Maßnahmen werden definiert, aber nicht systematisch nachgehalten. Fristen geraten aus dem Blick, Prioritäten verschieben sich und Eskalationspfade fehlen. Statt eines gesteuerten Prozesses entsteht eine leblose Sammlung offener Aufgaben.
- **Unklare Verantwortlichkeiten & Silodenken**
  Auch wenn Rollen formell vergeben sind, fehlt im Alltag die operative Klarheit. Da NIS2 und BCM bereichsübergreifende Themen sind, führen Schnittstellenprobleme zwischen IT, Security und den Fachbereichen zu Verzögerungen oder Doppelarbeit.
- **Auditfähigkeit nur auf Abruf**
  Nachweise werden häufig erst dann mühsam zusammengestellt, wenn der Auditor vor der Tür steht. Das führt zu Stress, Unsicherheit und im schlimmsten Fall zu Lücken in der Dokumentation.
- **Fragmentierte Prozesse ohne Synergien**
  ISMS, BCM und Datenschutz laufen oft in isolierten Parallelwelten. Informationen müssen manuell übertragen werden, Synergien (zum Beispiel zwischen der Risikoanalyse im ISMS und der Business Impact Analyse im BCM) bleiben ungenutzt.

Der blinde Fleck: Diese Probleme treten nicht auf, weil die regulatorischen Anforderungen missverstanden werden, sondern weil der Faktor Mensch (Ressourcenengpässe) und die kontinuierliche Governance im Alltag fehlen.

Der entscheidende Perspektivwechsel: Compliance ist kein Projekt.

Der zentrale Fehler liegt darin, Governance, Risk und Compliance (GRC) als einmaliges Projekt mit einem definierten Enddatum zu betrachten. NIS2 und BCM sind jedoch kontinuierliche Steuerungsprozesse. Hier ist dient die Haftung als Treiber. Insbesondere bei NIS2 steht das Top-Management in

*/ Der zentrale Fehler liegt darin, Governance, Risk und Compliance (GRC) als einmaliges Projekt mit einem definierten Enddatum zu betrachten.

der Pflicht. Die Geschäftsführung haftet persönlich für die Implementierung und Überwachung der Risikomanagement-Maßnahmen, dieser Tragweite ist sich die Chefetage oft nicht bewusst. Ein reines »Abhaken« von Checklisten oder die Übertragung der Zuständigkeit auf den CISO reicht rechtlich nicht aus.

Organisationen, die den Schritt von der Papier-Compliance zur echten Resilienz erfolgreich gehen, richten ihre Strukturen entlang von vier Prinzipien aus:

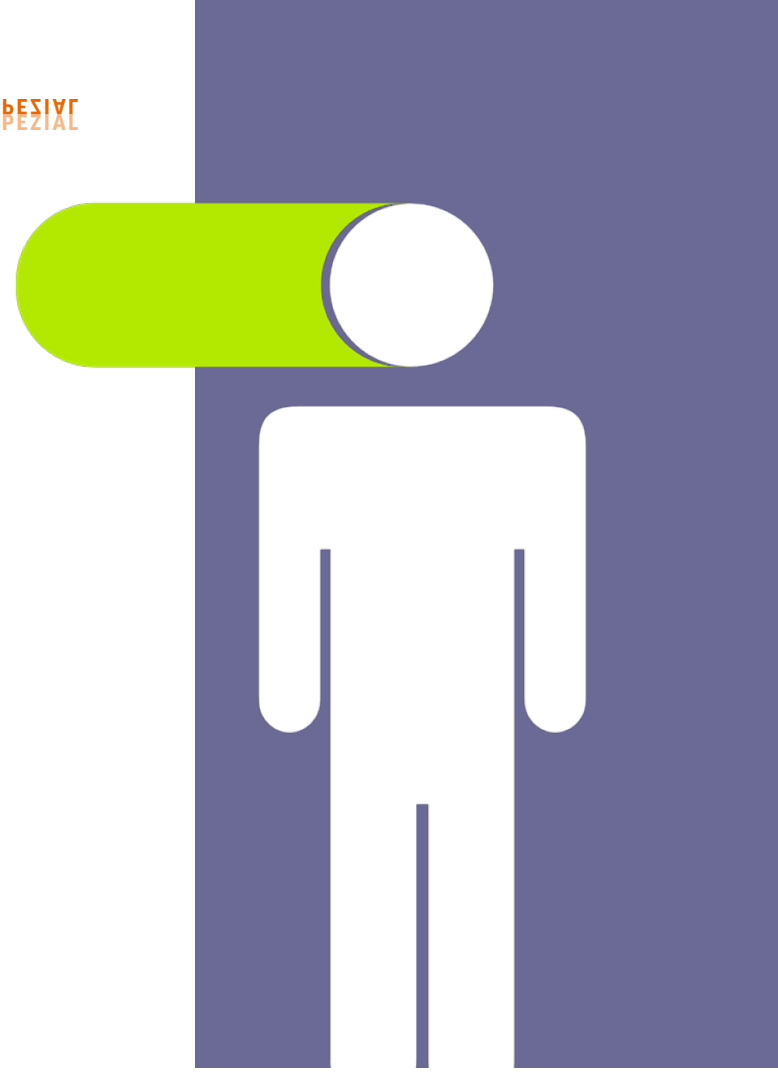
- **Transparente Gesamtstruktur schaffen**
  Alle relevanten Informationen – Risiken, Maßnahmen, Nachweise – müssen zentral, vernetzt und ohne Medienbrüche verfügbar sein.
- **Verantwortlichkeiten in die Breite tragen**
  Die Verantwortung gehört weg von solitären »Beauftragten« (wie dem CISO) und hin zu den Prozessverantwortlichen in den Fachbereichen. Wer die operative Maßnahme verantwortet, muss auch für deren Freigabe und Nachweiserbringung zuständig sein.
- **Maßnahmen aktiv und agil steuern**
  Fristen, Status und Fortschritt müssen über Dashboards sichtbar sein. Ohne ein funktionierendes Eskalationsmanagement bleibt die Umsetzung dem Zufall überlassen.
- **Auditfähigkeit als Dauerzustand (Continuous Auditing)**
  Nachweise sollten als Nebenprodukt des täglichen Arbeitens entstehen, nicht als Sonderaufgabe für das Audit. Ziel ist ein Zustand, in dem die Organisation jederzeit prüfungsbereit ist.

Was das für die Praxis bedeutet. Der entscheidende Mehrwert entsteht dort, wo Informationssicherheit, Business Continuity und Risikomanagement nicht länger als getrennte Disziplinen betrachtet werden. Erst wenn diese Bereiche miteinander verzahnt sind, lassen sich Risiken realistisch bewerten, Maßnahmen gezielt priorisieren und Verantwortlichkeiten eindeutig steuern.

Wenn Organisationen diesen Perspektivwechsel vollziehen, profitiert das gesamte Unternehmen:

- **Integrierte Durchführung von BCM und BIA:** Business Impact Analysen (BIA) und Notfallplanungen erfolgen nicht mehr isoliert. Die Ergebnisse der BIA fließen direkt in die Risikobewertung des ISMS ein und steuern die Priorisierung von IT-Sicherheitsmaßnahmen.
- **Nachvollziehbare Maßnahmenumsetzung:** Ob NIS2Anforderung oder interne Richtlinie: Jede Maßnahme ist klar zugewiesen, ihr Status ist transparent und Fortschritte lassen sich lückenlos historisieren.
- **Entlastung beim Audit:** Statt Unterlagen kurzfristig zusammenzusuchen, sind alle Nachweise strukturiert hinterlegt. Prüfungen werden planbar und verlieren ihren Schrecken.

Organisationen gewinnen dadurch nicht nur Sicherheit, sondern auch Effizienz. Prozesse werden robuster, Abhängigkeiten transparenter und Entscheidungen besser fundiert. Gleichzeitig entsteht eine belastbare Grundlage, um regulatorische Anforderungen kontinuierlich zu erfüllen und die eigene Widerstandsfähigkeit nachhaltig zu stärken.



Fazit: Organisation und System müssen zusammenspielen. Viele Organisationen haben erkannt, dass Excel-Tabellen und fragmentierte Einzeltools für die komplexen Anforderungen von NIS2 und modernem BCM nicht mehr ausreichen. Eine Tool-Einführung allein löst das Problem jedoch nicht. Software kann Prozesse abbilden und automatisieren – sie ersetzt jedoch nicht die organisatorische Klarheit und den Kulturwandel im Unternehmen.

Wer NIS2, BCM und ISM nachhaltig und haftungssicher umsetzen möchte, sollte den Fokus weg von der reinen Dokumentation und hin zur kontinuierlichen Steuerungsfähigkeit der eigenen Organisation lenken. Genau hier entscheidet sich, ob aus Papier-Compliance echte digitale Resilienz entsteht.

Silke Menzel,
Consultant Projektmanagement,
HiScout