

Friederike Krüsemann
Henning Heuter

REIFEGRADE IM INTERNEN KONTROLLSYSTEM

AUSFÜHRLICHES FALLBEISPIEL

EINLEITUNG

Der häufigste Grund für überdimensionierte Kontrollen ist eine unzureichende Verknüpfung zwischen der Risikoanalyse und dem Kontroll-Design. Kontrollen dürfen niemals im luftleeren Raum entstehen, sondern müssen direkt aus einer fundierten Bewertung der inhärenten Risiken (Risiko vor Kontrollen) abgeleitet werden.

Im vorherigen Beitrag *Qualität vor Quantität im IKS – Wie das interne Kontrollsystem risikoorientiert ausgestaltet werden kann* wurden die Herausforderungen, das IKS als strategisches Steuerungsinstrument zu formen, herausgearbeitet. Dieser Beitrag beschäftigt sich ausführlich mit einem Lösungsansatz, das Risiko vor Kontrolle konsequent mit den eingesetzten Kontrollen zu verknüpfen, um ein zielgerichtetes und effizientes IKS zu gewährleisten. Ziel ist es, Risiken in dem Ausmaß zu kontrollieren, wie es sinnvoll und notwendig ist. Vermieden werden soll, dass Risiken zu wenig oder auch zu viel kontrolliert werden, um die Wirtschaftlichkeit zu sichern.

WAS BEDEUTET REIFEGRAD- MODELL?

Eine Möglichkeit dafür bietet das Reifegradmodell. Voraussetzung für die Anwendung des Reifegradmodells ist eine monetäre Bewertung jedes Risikos. Eine Bewertung in monetären Gruppen (bspw. niedrig – bis 5.000 EUR, hoch – bis 15.000 EUR) muss gut durchdacht sein und evaluiert werden. Das Risikopotenzial vor Kontrolle setzt sich zusammen aus der Eintrittshäufigkeit und der Schadenshöhe vor Kontrolle ($\text{Risikopotenzial vor Kontrolle} = \text{Eintrittshäufigkeit} * \text{Schadenshöhe vor Kontrolle}$). Sprich, ein Risiko, welches eine sehr große Schadenshöhe zur Folge hätte, kann trotzdem ein recht niedriges Risikopotenzial aufweisen, wenn die Eintrittshäufigkeit sehr gering ist.

Hinweise zur Bewertung des Risikos werden im weiteren Verlauf des Fachbeitrags vorgestellt.

EINZELSCHRITTE FÜR DAS REIFE- GRADMODELL

Das Reifegradmodell beinhaltet folgende Schritte:

1. Jedes Risiko wird mit einem Risikopotenzial vor Kontrolle bewertet.
2. Das Risiko wird nach der Reifegradmatrix (s.u.) eingeordnet. Somit sind die Anforderungen an notwendige Kontrollen ersichtlich.
3. Bereits etablierte Kontrollen werden mit den Anforderungen abgeglichen. Es gibt drei Möglichkeiten:
 - a. die etablierten Kontrollen passen genau zu den Anforderungen → keine Handlung notwendig
 - b. die etablierten Kontrollen sind zu stark, die Anforderungen werden übertroffen → Evaluierung, ob Kontrollen eliminiert werden können
 - c. die etablierten Kontrollen sind nicht ausreichend, die Anforderungen werden nicht getroffen → Es müssen neue Kontrollen implementiert werden
4. Das Risikopotenzial nach Kontrolle wird bewertet: Wie stark lässt sich das Risiko durch die Maßnahmen verringern?

REIFEGRAD- MODELL: WESENTLICH- KEITSGRENZE

Institute müssen klare, quantifizierte Toleranzschwellen festlegen. Liegt der maximale potenzielle Schaden eines Risikos vor Kontrolle unter der Wesentlichkeitsgrenze, ist eine engmaschige, manuelle Kontrolle gegebenenfalls wirtschaftlich nicht zu rechtfertigen. Es gibt verschiedene Möglichkeiten, die Wesentlichkeitsgrenzen festzulegen. So können absolute Beträge definiert werden (s. Tabelle unten), es besteht aber auch die Möglichkeit, einen prozentualen Anteil

- vom Vorjahresgewinn oder
- des Risikodeckungspotenzials oder
- des Businessindikators des Standardansatzes

anzunehmen.

BEWERTUNG RISIKO VOR KONTROLLE

Das Einführen von konkreten monetären Bewertungen (Risikopotenzial) kann initial aufwendig sein und auf Widerstand stoßen.

Achtung: Es handelt sich um das Risiko VOR Kontrolle. Bei der Bewertung dürfen also keine Kontrollen, die das Risiko bereits verringern, beachtet werden. Es muss unter der Annahme, dass keinerlei Kontrollen vorliegen, bewertet werden.

Gute Ansatzpunkte für schwer zu bewertende Risiken sind Personenstunden, die für eine Bereinigung anfallen, oder potentielle Strafzahlungen. Ebenso sollte beachtet werden, ob die Aufgabe, die hinter dem Risiko liegt, Einfluss auf Vorstandsentscheidungen hat oder eine Datenbasis für anderweitige Entscheidungen darstellt. Zu dem Zweck sollte stets hinterfragt werden, was in weiterer Folge im Prozess passieren kann, wenn das Risiko eintritt. Dies sollte auch in die Bewertung einfließen.

Als Beispiel nehmen wir das Erstellen eines Risikoberichts. Sollte der Bericht fehlerhaft sein, werden keine direkten Strafzahlungen fällig und auch die Personenstunden, um die Fehler auszubessern, belaufen sich annahmegemäß auf etwa 2 Stunden. Demnach scheint das Risiko auf den ersten Blick gering. Interessant wird es, wenn man den Prozess im weiteren Verlauf anschaut: Der Bericht geht an den Vorstand, der auf dessen Basis weitreichende Entscheidungen trifft. Jetzt sieht

es auf einmal anders aus und das Risiko kann doch zu eklatanten Schäden führen. Mit diesem Wissen im Hintergrund, sollte eine angemessene Schadenshöhe definiert werden.

Jeder Risikobericht ist entscheidungsrelevant, für die Bestimmung der potenziellen Schadenshöhe sollte analysiert werden, welche Art von Informationen der konkrete Bericht liefert und welche Entscheidungen daraus abgeleitet werden. Geht es um Investitionen, Kreditvergabeentscheidungen oder die Freigabe künftiger Mitarbeiterstellen? Was kann passieren, wenn bspw. eine Investition nicht erfolgreich ist? Wie hoch ist die durchschnittliche Investitionssumme im Institut?

Einerseits geht es hier um direkte finanzielle Einbußen, andererseits auch um die Frage, ob eine Fehlentscheidung zu einem Reputationsschaden führen kann, der einbezogen werden muss. Der Personalaufwand zum Handling bzw. der Behebung sollte ebenfalls wie oben beschrieben inkludiert werden.

Wichtig ist es, dass ein durchschnittliches Schadenspotenzial gesucht werden sollte, welches möglichst viele Szenarien abdeckt. Ein Anspruch auf Vollständigkeit sollte und kann realistisch betrachtet gar nicht vorhanden sein. Damit das Konzept der Reifegrade für den Arbeitsalltag tauglich ist, muss es möglichst einfach und händelbar bleiben.

Fokus auf das Risiko nach Kontrolle (Restrisiko): Ziel einer Kontrolle ist es, das inhärente Risiko auf ein akzeptables Restrisiko-Niveau zu senken. Ist das Risiko ohnehin gering, reicht oft eine Basisüberwachung oder die bewusste Akzeptanz des Risikos aus.

Es ist nicht grundsätzlich das Ziel, ein Risiko zu eliminieren. Ebenso kann ein Risiko akzeptiert, übertragen oder reduziert werden. Dies hängt von der Schwere des Risikos, aber auch vom Risikoappetit und dem Geschäftsmodell ab und ist häufig eine Managemententscheidung.

Zusammengefasst bedeutet das, dass vor der Etablierung von Kontrollen das Risiko vor Kontrolle bewertet werden muss. Die Höhe dieses Risikos bzw. Schadens wird mit den Wesentlichkeitsgrenzen abgeglichen, woraus bestimmte Kriterien für eine Kontrollgestaltung folgen. Nun gilt es zu bestimmen, welchen Einfluss die gesetzten Kontrollen auf das Risiko haben. Die Schadenshöhe an sich wird sich nicht ändern. Tritt ein Risiko ein, tritt es genauso ein als wenn es keine Kontrollen gäbe. Was hingegen beeinflussbar ist, ist die Eintrittshäufigkeit. Die Kontrollen sollten bewirken, dass ein Risiko deutlich seltener eintritt als ohne Kontrollen, was das Schadenspotenzial nach Kontrolle (= Schadenshöhe * Eintrittshäufigkeit) vermindert.

Im Folgenden wird ein Beispiel skizziert, wie eine solche Gestaltung aussehen könnte:

Wesentlichkeitsgrenze/ Risikopotenzial vor Kontrolle	Reifegrad 1	Reifegrad 2	Reifegrad 3	Reifegrad 4	Reifegrad 5
< 5.000 EUR	X				
5.000 – 15.000 EUR		X			
15.001 – 25.000 EUR			X		
25.001 – 35.000 EUR				X	
> 35.000 EUR					X

Tabelle 1: Reifegradmatrix

REIFEGRAD- MODELL: RISIKO NACH KONTROLLE

REIFEGRAD- MATRIX

Die Reifegrade stellen einen Mindestreifegrad dar, sprich sie dürfen nicht unterschritten werden. Wenn die Kontrollen den Reifegrad überschreiten, ist dies in Ordnung, sollte aber hinterfragt werden. Dieser Fall wird weiter unten im Beitrag diskutiert.

Anforderungen an die Reifegrade

Reifegrad 1: Stichprobenartige präventive Kontrollen des ausführenden Mitarbeiters

Die Qualitätssicherung liegt hauptsächlich bei der ausführenden Person, weswegen es sich hier um die niedrigste Stufe der Reifegrade handelt. Es wird eine große Eigenverantwortung, eine genaue Arbeitsweise und ausreichendes Fachwissen vorausgesetzt. Bevor der Mitarbeiter den Prozessschritt abschließt, kontrolliert er die eigene Arbeit stichprobenartig auf Fehler. Es gibt weder Zeitpläne noch starre Vorgaben oder Dokumentationspflichten. Seine eigene Arbeit zu kontrollieren, sollte das Minimum an Kontrolle darstellen.

Schwächen dieses Reifegrades liegen in der Personenabhängigkeit und dass eigene Fehler schneller übersehen werden. Je nach Arbeitsbelastung kann auch die Genauigkeit steigen oder sinken.

Reifegrad 2: Stichprobenartige präventive Kontrollen im Vier-Augen-Prinzip, standardisierte Dokumentation notwendig

Im Gegensatz zu Reifegrad 1 kommt bei dieser Stufe eine zweite Person ins Spiel. Es handelt sich nicht um eine vollständige Kontrolle, sondern um eine Stichprobe. Der Umfang der Stichprobe muss vorher definiert werden. Die Auswahl der Kontrollstellen kann sich nach dem Zufallsprinzip richten oder in bestimmten Intervallen erfolgen.

Ein weiterer Qualitätsunterschied zu Reifegrad 1 liegt in der Dokumentation. Jede Kontrolle muss entweder über eine Checkliste oder ein Protokoll erfasst werden.

Auch die größte Schwäche des ersten Reifegrads wird umgangen: Durch das Einbinden einer zweiten Person werden die Kontrollen genauer.

Reifegrad 3: Vollständige präventive Kontrollen im Vier-Augen-Prinzip, standardisierte Dokumentation notwendig, wird auf aggregierter Datenbasis auf Wirksamkeit geprüft

Reifegrad 3 geht noch einen Schritt weiter und setzt auf eine vollständige Kontrolle. Jeder Vorgang wird von einer zweiten Person geprüft, was dokumentiert wird. Die Kontrolle wird auf ihre Wirksamkeit überprüft, indem die Ergebnisse auf aggregierter Ebene zusammengefasst und analysiert werden. Sollte auf dieser aggregierten Ebene ein Fehler festgestellt werden, müssen diese Daten erneut auf Einzelebene überprüft werden. Beachtet werden sollte der Sonderfall, dass sich zwei Fehler, die in der gleichen Datenbasis auftreten, gegenseitig ausgleichen können und deshalb nicht auffallen.

Der Reifegrad 3 führt zu einer sehr hohen operativen Sicherheit. Durch die Dokumentation kann nachvollzogen werden, wie die Prozesse ausgestaltet und wo Fehleranfälligkeiten zu finden sind.

Reifegrad 4: Vollständige präventive Kontrollen im Vier-Augen-Prinzip, standardisierte Dokumentation notwendig, wird auf Einzeldatenbasis auf Wirksamkeit geprüft

Der Reifegrad 4 unterscheidet sich zum Reifegrad 3 dadurch, dass die Wirksamkeit von Anfang an auf Einzelebene überprüft wird. So wird eine detaillierte Nachverfolgung und Analyse gewährleistet und ein Fehlerausgleich untereinander ausgeschlossen. Da diese Art von Kontrolle einen sehr

hohen personellen Aufwand erfordert, sollte der Reifegrad 4 nur bei sehr hohen Risiken eingesetzt werden.

Reifegrad 5: Automatisierte Kontrolle muss eingeführt werden

Der Reifegrad 5 ist die höchste Kontrollstufe. Nach erfolgreicher Implementierung und abgesehen von etwaigen Wartungen und Anpassungen kann eine Eliminierung des Faktors Mensch erreicht werden. Trotz hoher Sicherheitsstufen und genauer Kontrolle kann von Menschen nicht immer eine 100%ige Trefferquote erwartet werden.

Systemseitige, automatisierte Kontrollen sorgen dafür, dass Fehler oder unzulässige Arbeitsschritte direkt unterbunden werden. Das Einführen solcher automatischen Kontrollen ist allerdings oftmals sehr langwierig und kostenintensiv, auch die laufende Systempflege kann viele Ressourcen beanspruchen.

Ein weiterer Aspekt, der beachtet werden muss, ist die Flexibilität von Prozessen im Gegensatz zu starren Vorgaben bei automatisierten Kontrollen. Nicht jede Kontrolle lässt sich über eine Automatisierung abbilden oder verursacht bei der Implementierung hohe Aufwände.

Es muss gut abgewogen werden, ob der Implementierungsaufwand im Gegensatz zum Vier-Augen-Prinzip lohnenswert ist oder ob es technische Restriktionen gibt, die eine automatisierte Kontrolle quasi unmöglich machen. Sollte das Fazit gezogen werden, dass der Reifegrad 5 nicht umsetzbar ist, muss intern ein individuelles Konzept zum weiteren Vorgehen vorliegen. Weitere Gedanken dazu folgen im nächsten Kapitel.

Wie die konkrete Ausgestaltung der Reifegrade aussieht, sollte institutsabhängig entschieden und abhängig von den finalen Wesentlichkeitsgrenzen sein.

Nach der Festlegung der Reifegrade und Wesentlichkeitsgrenzen, gibt es noch einige Überlegungen zu tätigen:

Wie geht das Institut damit um, wenn der Mindestreifegrad deutlich überschritten wird?

Grundsätzlich sollte jedes Risiko aus wirtschaftlichen Gründen genau so intensiv kontrolliert werden, wie es der Reifegrad vorgibt. Besonders Kontrollen im Vier-Augen-Prinzip kosten sehr viel Arbeitszeit und sollten nur dort eingesetzt werden, wo sie notwendig sind. Etwas anders verhält es sich mit dem Reifegrad 5 aus unserem Beispiel. Sind automatisierte Kontrollen einmal eingeführt, binden sie kaum Arbeitszeit. Zu prüfen sind dort die Kostenaspekte und der Zeitaufwand für eine etwaige Auswertung. Eine automatisierte Kontrolle mit geringen Kosten und kaum Aufwand sollte nicht ohne Not wieder eliminiert werden.

Wird das Vier-Augen-Prinzip wirklich gelebt?

Erfahrungsgemäß wird vielen Risiken mit Kontrollen im Vier-Augen-Prinzip begegnet. Die tatsächliche Umsetzung wird allerdings häufig aus verschiedensten Gründen vernachlässigt. So sind gründlich ausgeführte Vier-Augen-Kontrollen sehr zeit- und arbeitsintensiv. Das führt dazu, dass die Ausführung im Arbeitsalltag manchmal unbefriedigend ist: Pop-ups werden weggeklickt, der Arbeitskollege unterschreibt blind die Korrektheit oder der Vorgesetzte vertraut auf seine Mitarbeiter.

Es gibt jedoch Tätigkeiten, bei denen es sehr sinnvoll ist, dass eine zweite Person die Arbeit kontrolliert. Um zu gewährleisten, dass diese Kontrolle korrekt ausgeführt wird, sollte das Vier-Augen-

WEITERE ÜBERLEGUNGEN

Prinzip nicht zum Allheilmittel werden. Eine Sensibilisierung aller Mitarbeiter, was ein Vier-Augen-Prinzip wirklich umfasst, ist unerlässlich.

Was ist zu tun, wenn eine automatisierte Kontrolle nicht möglich ist?

Eine automatisierte Kontrolle kann aus verschiedenen Gründen nicht umsetzbar sein. So können beispielsweise technische Restriktionen vorliegen, zu viele Sonderfälle existieren oder der Entscheidungsprozess zu komplex sein, als dass er sich technisch darstellen lässt. Für diesen Fall gilt es, sich institutsintern eine Lösung zu überlegen.

Gesondert aufgreifen möchten wir den Reifegrad 4: Er ist qualitativ sehr hochwertig, bindet aber gleichzeitig sehr viele Personalressourcen. Die Weiterentwicklung zu Reifegrad 3 ist zwar vorhanden, bezieht sich aber (nur) auf das Aggregationslevel, auf dem geprüft wird. So könnte man überlegen, ob Reifegrad 3 der maximale Mindestreifegrad ist und Reifegrad 4 und 5 eher als Empfehlung gesehen werden. Sprich, selbst wenn ein Risiko im obigen Beispiel ein Schadenspotenzial über 35.000 EUR aufweist, genügt das Einführen von Kontrollen, die dem Reifegrad 3 entsprechen. Es sollte aber geprüft werden, ob eine automatisierte Kontrolle möglich oder ob eine Wirksamkeitsprüfung auf Einzeldatenbasis sinnvoll ist. So wird sichergestellt, dass das Reifegradmodell für den Arbeitsalltag tauglich bleibt.

Sollen besondere Regelungen für vorstandsrelevante Risiken gelten?

Wie oben diskutiert, haben einige Prozesse weitreichende Auswirkungen, vor allem, wenn sie vorstandsrelevant sind. Eine Möglichkeit wäre, pauschal für Prozesse mit Vorstandsrelevanz einen Reifegrad von 3 oder 4 festzulegen.

Sie möchten noch mehr im Zusammenhang mit Reifegraden im IKS wissen oder mit uns zu diesen Themen diskutieren? Die 1 PLUS i GmbH unterstützt Sie neben der Klärung spezifischer Fragen insb. auch bei der konkreten Gestaltung der Reifegradmatrix, der Einführung jener inkl. aller notwendigen Anpassungen im IKS und bei der Etablierung der neuen Perspektive. Wir erarbeiten u.a. individuelle Konzepte, welche wir Ihnen in Form von Inhouse-Kundenworkshops sehr gern vorstellen. Sprechen Sie uns doch einfach an!

Ihr 1 PLUS i Team



HENNING HEUTER
henning.heuter@1plusi.de



FRIEDERIKE KRÜSEMANN
friederike.krusemann@1plusi.de

UNTERSTÜTZUNG
DURCH 1 PLUS i

AUTOREN