

# 'Gefühletes RisikoAudit'

## Szenarium für die betriebliche Nutzung

einer elektronischen Bewertungshilfe kritischer Ereignisse

1. Ein betrieblicher Administrator (z. B. FASI oder autorisierte Führungskräfte) stellt eine Unfallbeschreibung, Verbandbucheintragung oder einen Beinaheunfall in das System ein und verlinkt es mit dem hauseigenen Intranet (Foto + Kurzbeschreibung).
2. Mitarbeiter des Unternehmens, denen die gleiche Gefährdung wiederfahren kann, werden aufgefordert, die dargestellte Situation zu bewerten.
3. Der/die Bereichsleiter der betroffenen Einheit(en) werden per E-Mail oder verbal gebeten die eignen Mitarbeiter innerhalb eines Aktionszeitraums von z. B. 3 Wochen bewerten zu lassen. (Mitarbeiter ohne eigenen Netz-Anschluss erhalten Zugang über einen zentralen Terminal.)
4. Die betroffenen Mitarbeiter geben im Aktionszeitraum Ihr persönliches Votum ab und erhalten umgehend die Durchschnittswerte der zuvor abgegebenen Voten sowie eine Meldung zur Dringlichkeit einer Handlung. Starke Abweichungen der persönlichen Einschätzung einzelner Mitarbeiter vom Durchschnitt aller Teilnehmer führen automatisch zur Selbstreflektion bzw. zur Diskussion.
5. Dem Bediener wird die Möglichkeit geboten, eine Lösungsmöglichkeit vorzuschlagen. (Es kann eingerichtet werden, dass nach dem Aktionszeitraum alle Ideen als PDF an das 'Betriebliche Vorschlagswesen' gesandt werden.)
6. Es kann eingerichtet/programmiert werden, dass nach überschreiten definierter Durchschnittszahlen (vom Administrator zuvor einstellbare Grenzwerte), automatisch Warnmeldungen (PDF) an die handlungsrelevanten Personen gehen (z. B.: Abteilungsleiter bei 10, Betriebsleiter bei 40, Geschäftsführung bei 90).
7. Um einen kollektiven Irrtum entgegenzutreten wird ein Expertenvotum hinterlegt
8. Als Argumentationshilfe für Vorgesetzte werden Fachinformationen hinterlegt
9. Der direkte Vorgesetzte wird gebeten mit den Ergebnissen der Bewertung eine Unterweisung durchzuführen und sich nach Möglichkeit mit den Teilnehmern auf eine akzeptierte Lösung zu verständigen.

10. Nach Ende des Aktionszeitraumes kann die jeweilige Führungskraft den Prozess managen. Das System kann erweitert werden, so dass der verantwortliche Akteur, die zur Bearbeitung erforderlichen Personen ins System eingibt. Ein PDF wird automatisch an die relevanten Personen versandt, die den Auftrag erhalten, die Verbesserungsmaßnahme umzusetzen.
11. Optional wird durch möglichst viele der betroffenen / beteiligten Personen ein Termin vor Ort vereinbart. Innerhalb dieses Gesprächs werden technische, organisatorische Maßnahmen geprüft, die Situation zu entschärfen bzw. sie mindestens in den gelben oder grünen Bereich der Bewertungsskala zu transferieren.
12. Wird **keine** schnelle wirtschaftliche Lösung gefunden, wird unter Einbeziehung aller Beteiligten ein Verhaltenskodex vereinbart, wie mit dieser Situation in Zukunft umgegangen wird.

## Effekte des 'Gefühlten RisikoAudits'

Das 'Gefühlte RisikoAudit' ist eine vereinfachte Methode auf der Basis der Gefährdungsbeurteilung nach Nohl. Das System gestattet die gesetzlich geforderte Beteiligung der Mitarbeiter. Der Gedanke '**häufig**' (Eintrittswahrscheinlichkeit) multipliziert mit '**heftig**' (Schadensausmaß) erfährt Verbreitung in der Belegschaft. Die Bewertung eines Risikos aus dem Durchschnittswert der Betroffenen weist ein einigermaßen realistisches Ergebnis aus.

Nach der Erkenntnis: >Die Risikoeinschätzung bestimmt das Vorsorgeverhalten< wird bei einer allgemeinen Erhöhung der Risikoeinschätzung (s. Position 7) das Vorsorgeverhalten der Mitarbeiter steigen. Unterschätzen Teilnehmer den Durchschnittswert erheblich, steigt die Wahrscheinlichkeit, dass es irgendwann schief geht. Durch den Vergleich mit dem Durchschnittswert der Gruppe, erfolgt eine Verunsicherung und damit die Chance des Abgleichs auf ein realistisches Niveau. Die Wahrscheinlichkeit verringert sich, dass ein kritisches Ereignis zu einem Schaden führt. Kommt es durch erhöhte Aufmerksamkeit nicht zu kritischen Ereignissen, verringert sich im Laufe der Zeit das Bewusstsein für die Gefährdung wieder.

Erfolgt vom Management keine Reaktion auf die Bekanntgabe eines von allen Beteiligten als 'hoch' eingeschätzten Risikos (s. Position 6), entsteht ein Problem für die Leitung, wenn innerhalb eines überschaubaren Zeitraums tatsächlich ein unerwünschtes Ereignis eintritt.

Das Programm und die zugehörigen Datenbanken werden auf einem zentralen Server installiert. Ein Startbutton im Intranet des anwendenden Unternehmens startet den Zugang. Alle Daten werden verschlüsselt gesendet und sind nur über ein dem Unternehmen zugewiesenen Login einsehbar.