

# Erfolgsfaktoren des Krisenmanagements

1. Krisenprävention
2. Krisenstab
3. Ausbildung des Krisenstabs
4. Alarmmanagement
5. Krisenbewältigung
6. Krisenkommunikation
7. Schutz von Betroffenen, Angehörigen und Mitarbeitern
8. Krisenmanagement-Handbuch
9. Nachbearbeitung von Krisenfällen
10. Krisenmanagement-Tools

Die nachfolgende Checkliste erhebt keinen Anspruch auf Richtigkeit und Vollständigkeit. Diese Checkliste muss firmenspezifisch angepasst werden. Secricon GmbH übernimmt infolgedessen keine juristische Verantwortung und wird keine daraus folgende oder sonstige Haftung übernehmen, die auf irgendeine Art aus der Benutzung der vorliegenden Checkliste oder Teilen davon entsteht.



## 1. Krisenprävention

- Die wirksamste Massnahme gegen eine Krise ist die Prävention.
- Nehmen der Aufsichtsrat / Verwaltungsrat sowie die Geschäftsführung ihre unternehmerische Verantwortung wahr?
- Werden Massnahmen zur Etablierung einer Fehlerkultur im Unternehmen seitens der Geschäftsführung gefördert und umgesetzt?
- Besteht ein Risikomanagementsystem, welches regelmässig die Risikosituation des Unternehmens erfasst und diese zielgruppenorientiert kommuniziert?
- Haben die Prozessverantwortlichen ihre Risiken nachweisbar im Griff?
- Ist das akzeptierbare Risiko und der Soll-Sicherheitsstandard definiert? Befinden sich alle Risiken im akzeptierbaren Restrisikobereich?
- Werden Gegenmassnahmen für die Risikohandhabung umgesetzt?

## 2. Krisenstab

- Sind die Mitglieder des Krisenstabs definiert?
- Sind die Rollen des Krisenstabs definiert und mit den richtigen Personen besetzt?
- Sind die Aufgaben, die Verantwortung und die Kompetenzen des Krisenstabs bestimmt?
- Ist der Krisenstab so erweiterbar, dass eine ereignisspezifische Zusammenstellung des Krisenstabs möglich ist?
- Kennen Sie externe Spezialisten, welche Sie im Ereignisfall unterstützen?

## 3. Ausbildung des Krisenstabs

- Werden regelmässig Krisenstabsübungen durchgeführt?
- Wurden der Krisenstab sowie relevante Einsatzteams in der Bewältigung von Krisensituationen ausgebildet?
- Führen Sie regelmässig Krisenstabsübungen / Planspiele zur Überprüfung der Funktionsfähigkeit Ihres Krisenmanagements durch?
- Werden die Ergebnisse der Krisenstabsübung protokolliert und im Krisenmanagement-Handbuch umgesetzt?
- Werden auch externe Journalisten, wichtige Lieferanten u. ä. in Krisenübungen integriert?
- Führen Sie regelmässig eine Alarmierung / Einberufung des Krisenstabs durch?
- Führt jedes Mitglied des Krisenstabs eine Liste der wichtigsten Telefonnummern bei sich?



### 4. Alarmmanagement

- Ist das Alarmmanagement dokumentiert?
- Ist das Kontaktverzeichnis aktuell, vollständig und an den relevanten Stellen verfügbar?
- Führen Sie regelmässig eine Alarmierung / Einberufung des Krisenstabs durch?
- Kennen Sie externe / behördliche Stellen, welche Sie in bestimmten Krisensituationen informieren müssen? Haben Sie mit diesen Stellen Kontakt?
- Führt jedes Mitglied des Krisenstabs eine Liste der wichtigsten Telefonnummern bei sich?

### 5. Krisenbewältigung

- Kennt der Krisenstab das Wertesystem des Unternehmens sowie das anderer relevanter Anspruchsgruppen und ist er in der Lage (Psyche, Kompetenz), dieses bei der Entscheidung kritischer Fragestellungen einzuhalten?
- Sind die relevanten Krisenszenarien bekannt?
- Haben Sie für die wichtigsten Krisenszenarien Krisenbewältigungspläne ausgearbeitet?
- Haben Sie die Krisenbewältigungspläne mit Ihren Kunden, externen Dienstleistern und Lieferanten abgestimmt?
- Sind die kritischen Ausfallzeiten wichtiger Prozesse und Prozessressourcen bekannt?
- Können kritische Ausfallzeiten während des Aufbaus des Notbetriebs bzw. der Disaster Recovery-Phase eingehalten werden?
- Gibt es Ausweichmöglichkeiten für wichtige Teilbereiche der Wertschöpfungskette?
- Wissen Sie, wie Sie bei einem nicht vorhersehbaren Ereignis agieren müssen?
- Haben Sie einen Krisenstabsraum, welcher den besonderen Anforderungen einer Krise genügt?
- Ist eine rechtssichere Sammlung und Archivierung versicherungsrelevanter und forensischer Informationen gewährleistet?

### 6. Krisenkommunikation

- Haben Sie eine interne / externe Krisenkommunikationsstrategie?
- Sind Sie in der Lage, eine Pressekonferenz durchzuführen bzw. eine Pressemitteilung zu veröffentlichen?
- Haben Sie vorgefertigte Pressemitteilungen erstellt, welche rasch an spezifische Ereignisbedingungen angepasst werden können?
- Haben Sie eine Dark Site für die rasche Kommunikation des Ereignisses über den Internetauftritt?
- Ist für den Krisenfall definiert, wer wem, was, wie kommuniziert sowie wer nicht kommuniziert?



### 7. Schutz von Betroffenen, Angehörigen und Mitarbeitern

- Sind die Mitarbeiter bezüglich des Verhaltens im Notfall ausgebildet?
- Sind die Mitarbeiter in Erster Hilfe ausgebildet? Gibt es einen Betriebsarzt?
- Haben Sie ein Evakuierungskonzept und ein ausgebildetes Evakuierungsteam?
- Werden Evakuierungsübungen durchgeführt?
- Sind Sie in der Lage, externe Einsatzkräfte aufzubieten? Wird das regelmässig geübt?
- Wissen Sie, was im Fall einer Geiselnahme, eines Amoklaufs, einer Bombendrohung zu tun ist und wo Sie Hilfe bekommen?
- Sind Sie in der Lage, eine professionelle Betreuung von Angehörigen durch professionelle Spezialisten zu initialisieren?
- Ist die Betreuung, Verpflegung des Krisenstabs im Ereignisfall organisiert?

### 8. Krisenmanagement-Handbuch

- Besitzen Sie ein aktuelles Krisenmanagement-Handbuch, welches für die Ausbildung des Krisenstabs geeignet ist?
- Wird das Krisenmanagement von der Internen Revision jährlich geprüft?
- Wird im Krisenmanagement-Handbuch klar zwischen Information, welche im Krisenfall relevant ist und solcher, welche für den Betrieb des Krisenmanagements benötigt wird, unterschieden?
- Kann im Ernstfall rasch auf Informationen, welche für die Krisenbewältigung benötigt werden, zugegriffen werden?
- Werden Krisenmanagement-Handbücher auch ausserhalb des Unternehmens / Standorts aufbewahrt?
- Ist das Krisenmanagement in andere Führungsinstrumente (Alarmorganisation, Werkschutz, Qualitätsmanagement, Risikomanagement) eingebunden?

### 9. Nachbearbeitung von Krisenfällen

- Ist dafür gesorgt, dass nach der unmittelbaren Krisenbewältigung, sowohl intern als auch extern eine Krisennachbearbeitung stattfindet und diese kommuniziert wird?
- Werden präventive Massnahmen für die zukünftige Vermeidung des Vorfalls entwickelt und umgesetzt?
- Wird die Effizienz und Effektivität des Krisenmanagements nach der Ereignisbewältigung geprüft und optimiert?
- Werden Krisenvorfälle bzw. Fast-Krisenvorfälle dokumentiert?



## 10. Krisenmanagement-Tools

Kennen Sie die Anwendungsgebiete von IT-gestützten Krisenmanagement-Tools?

Leistungen im Ereignisfall:

- Automatisierung des Alarmmanagements per E-Mail, SMS, Telefon, Gebäudealarmanlage;
- Kommunikationsplattform für geografisch verteilte Krisenstäbe / Einsatzteams;
- Entlastung des Krisenstabs bei der Informationsaufnahme (gleichzeitige Informationsgenerierung aller Beteiligten möglich);
- Automatische Protokollierung des Ereignisablaufs;
- Bereitstellung von entscheidungskritischen Informationen;
- Unterstützung des Krisenstabs bei der Planung der Krisenbewältigung;
- Automatisch generierte Statusberichte der Krisenbewältigung;
- Bewirtschaftung des Krisenmanagements;
- Dokumentenmanagement für das Krisenmanagement;
- Statusberichte über die Aktualität des Krisenmanagements;
- Workflows für die Bereitstellung und Aktualisierung des Krisenstabs;
- Generierung von Krisenmanagement-Handbüchern in unterschiedlichen Medien (Papier-Dokument, HTML (Intranet-Auftritt, DigiCard), Word-Bericht);
- Modellierung und Simulation von Krisenfällen für die Ausbildung des Krisenstabs.

Prüfen Sie:

- Haben Sie die Notwendigkeit eines IT-gestützten Krisenmanagementsystems geprüft?
- Erfüllt das ausgewählte Tool die Informationssicherheitsanforderungen (Verfügbarkeit, Vertraulichkeit, Integrität, Nachvollziehbarkeit der Informationen)?
- Ist das ausgewählte Tool benutzerfreundlich und in der Anwendung selbsterklärend?
- Hosten Sie das Tool im eigenem Unternehmen oder bei einem externen Hoster? Haben Sie die Integrität des externen Hosters geprüft? Erfüllt das Rechenzentrum des externen Hosters Ihre Sicherheitsanforderungen?

Prüfen Sie das Angebot an IT-gestützten Krisenmanagementsystemen genau, bevor Sie sich für eins entscheiden!