Whitepaper
Early Crisis Detection (ECD)

controllit
Business Continuity Management

Content

03
INTRODUCTION

04
DEFINITION AND TERMINOLOGY

06
NORMATIVE REQUIREMENTS

07
TYPES OF OPERATIONAL CRISES

8
USING EXISTING KEY FIGURES

11
INTEGRATION OF ECD INTO THE COMPANY

13
GOVERNMENTAL AND ECONOMIC DEVELOPMENTS

16
RECOMMENDATIONS FOR COMPANIES

18
SUMMARY

Introduction

Corporate crises rarely arise overnight. In most cases, the point of acute corporate problems or even the threat of insolvency is preceded by a longer history. Some crises already have a history within the company, which, if recognized in time, can make a crisis avoidable. The spectrum here ranges from liquidity bottlenecks to personnel and building deficiencies to IT challenges. Who does not remember the sometimes extremely delayed changeover from Windows 7 to the successor systems with correspondingly serious consequences? But also the currently necessary safeguards, e.g. through a solid processing of (security) patches and active geo-blocking to defend against cyber attacks, are part of it.

Because many companies lack an early warning system, they often find themselves in a crisis situation seemingly unawares. Once the crisis has occurred, the company's scope for action to counter the negative development is limited. Early crisis detection and prevention should therefore not be understood as a mere "new" duty of management, but rather as a valid means of ensuring the survival of companies, even beyond its strategic usefulness.

This white paper presents the information you need to do this and shows you how you can better position your organization with or without an existing crisis management system.

Definition and terminology

In the literature, two different definitions of the term can be found: Early warning and early detection.

(Crisis) early warning focuses on the analysis of potential hazards. In this respect, early warning is very closely related to risk management, which also involves the systematic identification and assessment of risks to a company's business operations.

In contrast, (crisis) early warning involves observing developments that could lead to crisis situations. In addition, in the context of early identification, an assessment is made as to whether they have the potential to develop into full-fledged crises and appropriate coping strategies and measures are planned. Thus, in addition to a pure warning function, early detection is based on the early recognition of opportunities and thus follows the objective of dealing with positive and negative future states.

The strategic foresight to identify emerging crises as early as possible, in order to be able to take preventive action in the best case, represents the core of early crisis detection. The risks and opportunities identified in this process can be evaluated in an established crisis management and/or business continuity management (BCM) system and used constructively to avert dangers.

Normative requirements

In addition to corresponding general and special legal regulations for the implementation of emergency, crisis and business continuity management measures, the idea of early detection of risks and crises has long been anchored in standards.

Section 91 (2) of the German Stock Corporation Act (AktG), which was introduced as part of the German Act on Corporate Control and Transparency (KonTraG), already stipulates that the Board of Management must take suitable measures and, in particular, set up a monitoring system to ensure that developments jeopardizing the continued existence of the Company are identified at an early stage.

Irrespective of the scope of this obligation and its applicability in relation to operational risks, the legislator now felt compelled to explicitly oblige the managers of limited liability companies to identify crises at an early stage and to manage them.

The Act on the Stabilization and Restructuring Framework for Companies (Gesetz über den Stabilisierungs- und Restrukturierungsrahmen für Unternehmen, Unternehmensstabilisierungs- und -Restructuring Act (StaRUG), represents a novelty for crisis managers simply because of the terminology chosen in the text of the law.

In Section 1 (1) Sentence 1 of the StaRUG, the legislator imposes a general duty on the management, across all legal forms, to keep a constant watch on economic and financial developments that could jeopardize the continued existence of the company (duty of early crisis detection). If endangering developments become apparent, the management must take suitable countermeasures in accordance with Section 1 (1) sentence 2 StaRUG (crisis management obligation) and immediately inform the bodies appointed to monitor the management of the emerging crisis. If the involvement of other bodies (e.g. the shareholders' meeting) is required to take the measures pursuant to Section 1 (1) sentence 2 StaRUG, the management is instructed pursuant to Section 1 (1) sentence 3 StaRUG to work towards their involvement without delay.

Normative requirements

The legislator and the guideline issuer have not laid down detailed requirements as to how the early detection of crises and crisis management are to be carried out.

It should also be noted that the law is systematically of a clearly insolvency law nature. Therefore, the question arises as to what types of crises are to be identified at an early stage in the eyes of the legislator. Insolvency law recognizes crisis terms under Sections 17-19 InsO, among others, namely insolvency, impending insolvency and overindebtedness.

These crisis concepts under insolvency law tend to be temporally downstream of operational crises, which are described in more detail in the following section.

Conversely, however, it seems sensible to understand the early crisis detection obligation as being sufficiently far forward in time so that, for example, crises can be countered such as those arising as a result of a cyber attack, a natural disaster or a production stoppage due to an acute gas shortage which is the result of a geopolitical dislocation. Impending insolvency or over-indebtedness may also prove to be a direct consequence of the latter.

The purpose of the standard, which is to anticipate crises at an early stage by means of analysis and to prompt management to act in a crisis at an early stage, argues that operational risks or crises in the areas covered by the scope of the early crisis detection obligation under Sec. 1 (1) StaRUG are also included.

Types of operational crises

Essentially, two types of crises can be distinguished for which companies can and should prepare: Acute crises and insidious crises. The so-called acute crises include all sudden events that can lead to a disruption of operations, such as

- Natural disasters, such as earthquakes, floods, hailstorms, etc.
- Financial crises, e.g. company or bank collapses
- Accidents
- Epidemics/pandemics, e.g. if a large part of the workforce is absent due to a wave of influenza
- Theft, fraud, industrial espionage
- Insolvency of important suppliers or customers

In contrast to acute crises, so-called creeping crises have a longer lead time and can often be recognized in advance. Nevertheless, the warning signs are often ignored for a long time until the effects have reached an unmistakably large scale. Creeping crises include, for example

- Increasing competitive pressure due to globalization and digitalization
- Restructuring
- Technical change
- Demographic change
- Shortage of skilled workers
- Political and social changes affecting production and/or operating business

Acute crises are rather rare. They require rapid action in an unexpected and often unknown situation. Creeping crises, on the other hand, often represent a permanent state to which people become so accustomed that the threshold to an acute crisis is often no longer perceived in time. Thus, an insidious, predictable and manageable crisis can turn into a seemingly acute emergency event. A preventive approach is recommended and, above all, possible, especially for creeping crises.

Using existing key figures

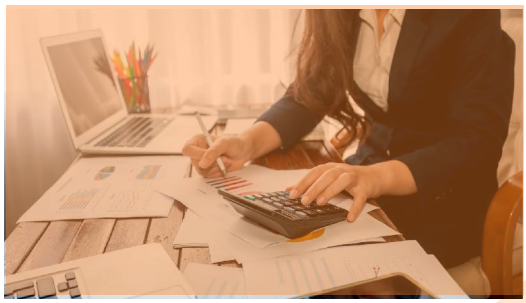
Warning signals can be identified for the events that have a high probability of occurring and that would have a strong impact on the companies. For each of these warning signals, a threshold value should be defined at which it can become critical so that countermeasures can be taken. Established crisis management systems often use these thresholds to establish an escalation process within the (crisis) organization. At this point, the early crisis detection of a company could therefore be well linked to the crisis management system. These warning signals can be very different: Sales figures, sick leave, crises in sales countries, political and social changes, innovations in the market, legal changes, etc.

Hard and soft factors can be used for the early detection of an impending corporate crisis. In the course of the company valuation, both sides must always be considered in order to be able to make a realistic assessment.

The **hard factors** are based on quantitatively verifiable figures. Usually, **annual financial statements**, **management reports** and **self-selected key figures** are used as a basis for verifying the current economic situation and making statements about the future development of the company.

Hard/quantitative factors of the ECD

- **Equity ratio**
- **Debt ratio**
- **Coverage ratio**
- **Debt-equity ratio**
- **Asset turnover**
- **Capital return ratio**



In addition, supplier and customer targets, inventory levels including supply chain considerations, and capital tied up in current assets should also be included in the analysis.

Using existing key figures

Soft factors (qualitative), on the other hand, are based on **information** and **observations** from management, employees and, if necessary, other external stakeholders. Management should have a clear strategy for dealing with observations, reports and incoming information in general. A regular and, at best, open exchange can help to identify negative developments at an early stage and to counteract them at an early stage. Another soft factor is the future viability of the company's own products.

Soft/qualitative factors of the ECD

- Fluctuation rate
- Sick leave
- Press reports
- Misunderstandings and rumors among employees
- pending legal disputes
- disputes within the circle of shareholders

A company should be constantly interested in improving its products and optimizing its processes. The same applies to the regular monitoring of costs and the use of funds. Most of the soft factors can be monitored and regulated conceptually by management, but appropriate implementation can only succeed in conjunction and in constant exchange with employees.

How is communication carried out internally and externally?
Which management style is chosen?
How are responsibilities distributed?
How are mistakes dealt with?

It is up to management to answer these questions, but it can only find the right answers in an exchange with its employees.

Using existing key figures

Established identification and survey procedures do not have to be changed completely, but can be adapted selectively. For example, numerous methods for identifying risks are proposed in the literature. A distinction is made between **collection methods** and **search methods**.

Collection methods are suitable for collecting obvious or already existing risks. This can be done, for example, using checklists, SWOT analyses, interviews or surveys. Search methods are used to proactively identify future risks. In addition to analytical methods such as question catalogs, failure mode and effect analyses, tree analyses or morphological methods, creativity techniques such as brainstorming, brainwriting, scenario analyses, synectics and the Delphi method are particularly helpful here.

Both methods offer starting points for the ECD, whereby in particular existing search methods can be taken up due to their anticipatory characteristic.

Integration of ECD into the company

ECD should not be carried out as an independent discipline within the company. Often, the factors and indicators described above for the early detection of negative corporate developments are already being collected, either consciously or unconsciously. Both the conservation of resources and the uniformity of the survey speak for an implementation of ECD based on established processes and disciplines.

Only when risks and requirements for the company are fully and correctly interpreted and their assessments are regularly processed on the basis of current information can the integration of ECD succeed in the best possible way.

Here, early crisis detection should be based on data from the following disciplines:

- Crisis Management (CM)
- Risk Management
- Business Continuity Management
- Controlling incl. supply chain consideration
- Human Resources
- Corporate Security (physical security/travel security)
- Compliance
- Corporate Communications
- Legal

An initial consolidation of the departments presented can consolidate the acceptance of ECD as an additional discipline within the company and classify its added value in relation to the departments presented. In this context, existing data and established surveys can be presented and synergies can be identified at an early stage. The ECD is significantly dependent on the support of other actors in order to dare a strategic view with their support, which can only be valid on the basis of a well-founded database.

For this purpose, a central point of contact and coordination is required, i.e., a specific functionary in the company who is ideally already responsible for CM or is at least at home in the other interface topics described above.

Integration of ECD into the company

ECD and crisis management

Crisis management focuses on ensuring a company's ability to make decisions and take action quickly in the event of any incident that poses a threat to the company. These capabilities are ensured primarily through organizational, personnel and material prevention. In order to plan this prevention and corresponding resources in the best possible way, information about potential crisis developments and their probability of occurrence is crucial. The generation, collection and analysis of this information using the interface and information management methods established in a crisis management system (CMS) can be ideally used for the ECD process. For this reason, the ECD has an essential partner in the company's CM. Early identification of crises or negative developments with crisis potential can have a significant impact on the structure, strategy, and resource requirements of reactive CM. Ideally, the ECD can use the possibilities of the KMS and/or BCM to stop precisely this negative development even before the crisis.

For this reason, the ECD should be integrated into all relevant phases and processes of the CM and represents a significant added value, especially in the proactive interface management of the responsible crisis manager. If the CM is based on a management cycle, it makes sense to link the ECD with the management in the individual cycle phases. To this end, it is advisable to review the current documentation and, if necessary, develop it further so that the process can be lived in all phases (including testing and rehearsal as a yardstick for accurate implementation).

Governmental and economic developments

Due to the fast pace of social and economic life and the seemingly unlimited potential for damage, there can be no absolute security today, neither for people nor for companies. However, the high level of technical dependency and the associated vulnerability also offer opportunities that can provide great added value for the early detection of crises. Anyone who wants to recognize where things are getting worse in the world or on which threats the current focus should be must keep an eye on the numerous data and media. In larger companies and public authorities, this media monitoring of established CMS is already systematically and professionally operated by crisis communication.

Artificial intelligence (AI) technologies are already capable of recording and processing diverse and massive data streams from sensors, cameras, weather stations and mobile networks and social media. This allows complex situations to be better understood, changes to be monitored in a timely manner, and unusual events to be detected.

On October 1, 2020, the German Federal Ministry of Defense (BMVg), together with the University of the Armed Forces Munich, launched a Competence Center Early Crisis Detection (KompZ KFE) as a pilot project at the university location in Neubiberg.

With the KompZ KFE, the Forum pushed the development of methodological expertise in the field of quantitative crisis and conflict research. It also contributes to the further development of special digital assistance systems that enable experts to recognize crisis potentials earlier and assess them better. These information technology tools process a wide range of information and data sources with recourse to advanced technologies (advanced analytics) in order to provide, among other things, forecasting information on the probability of crises escalating in different contexts.

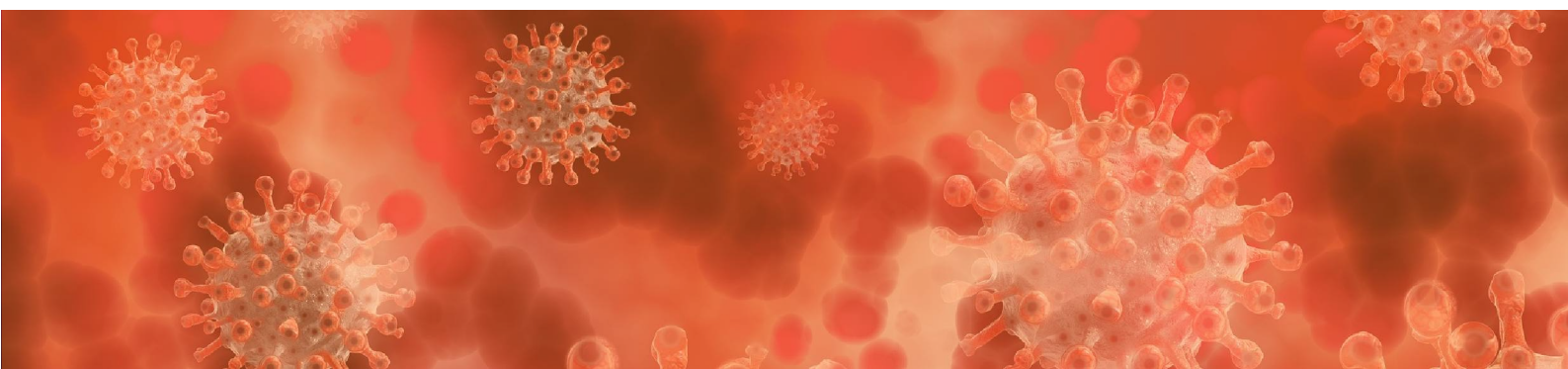
Governmental and economic developments

However, the task catalog of the KompZ KFE also includes the development and exploitation of synergy potentials between comparable instruments of the federal ministries, e.g. with regard to their interoperability or the joint use of suitable data for early crisis detection. The results of the KompZ KFE should also contribute to a more precise national situation picture and to the derivation of targeted recommendations for action - and thus also to preventive crisis management by the federal government. For this reason, other ministries should also have the opportunity to participate in the KompZ KFE on an equal footing, which could then also be accessible to companies in the medium term or indirectly.

The Bundeswehr's current **2016 White Paper** also attributes special importance to early crisis detection as a key capability feature. In the Bundeswehr, strategic foresight is used as a perspective analysis, assessment and planning tool. It is intended to capture (mega-) trends, construct scenarios, describe developments and capabilities, and provide target markers for long-term perspectives.

The qualitative factors presented above focus largely on company-related parameters. However, there are often unforeseen events and factors that would have been nice to recognize at an early stage. For these scenarios, the company and its employees are extensively prepared, for example in the context of a business continuity management system (BCMS) - even though the corresponding scenario occurs statistically every 10 years at most. It was also difficult to foresee the COVID 19 pandemic and the associated upheavals in the working world. One or the other company was prepared for this, as well as for rampages, terrorist attacks and natural disasters - at least on paper.

But how much more extensive could this preparation have been if the COVID 19 crisis had been recognized at an early stage and, above all, by many companies in a uniform manner?



Governmental and economic developments

The **Federal Foreign Office (AA)** uses the PREVIEW data tool to analyze publicly available data on the political, economic and social situation as well as on conflicts and violence for signs of crisis developments. PREVIEW uses various computer-based tools for this purpose. For example, visualizations such as information graphics with maps enriched with additional data make conflict situations visible and understandable at a glance. Trend analyses show the possible course of political and social developments and conflicts. Machine learning methods are also used to identify conflict and crisis patterns in large volumes of data. The results of these methods can help the Federal Foreign Office develop options for action and strategies for German crisis management.

The list could be continued with further analyses and recommendations from other authorities (police, fire department) and institutions. If you search a bit in your own environment with a concrete corporate perspective, you are sure to find systematic points of contact.

In addition to the strategic foresight of the military and foreign policy, private companies have already recognized the need for extended early warning. Services range from meeting legally-required minimum requirements to enterprise-wide provision of global current developments. From personal and individual on-site consultations to tool-supported databases that can be accessed via all end devices. The need and suitability here naturally depend on the individual company profile and the available resources of the company. Often, there are already strategic and tactical points of contact within the company, such as to the interface topics already described above and, in particular, to the media monitoring of an established crisis communication. A suitable path and scope for implementation is essential to properly integrate the company's already available data and actors and to ensure the usefulness, quality and targeting of the additional insights.

Recommendations for companies

- Review and communicate your commitment to early identification of emerging crises.
- Does early crisis detection perhaps already take place unconsciously? Whether it is in the minds of employees, management or in isolated conceptual developments - early crisis detection can begin with each individual employee in the context of the morning news report. Initial workshops could discuss this and raise awareness of the issue
- What information is already being collected and by whom? (e.g., crisis management, risk management, business continuity management, controlling incl. supply chain view, human resources, corporate security (physical security / travel security), compliance, corporate communications, legal)
- Which methods, contacts and sources for early detection of crises can be used? (Cooperation with local companies or companies in similar industries; reliance on situation reports from the states, federal government, etc.)
- Are risks identified in several areas of the company and does this result in synergies, savings potentials or extensions of the risk situation picture?
- What potentials and what need for adaptation are there in a joint consideration of the relevant areas (risk management, controlling, corporate security, etc.)?
- Which resources are necessary and available to integrate suitable information sources? (OSINT, internal/external risk monitoring, contacts with authorities, etc.).
- Have negative developments already been identified in the past and sensitized accordingly? Here, the topic could be made tangible for the company and a starting point for anchoring could be generated.

Recommendations for companies

- What insurance and reserves exist in case crises are not recognized in time?
- Can the existing crisis management be supplemented by early crisis detection, or do procedures need to be adapted here? Are there other suitable management systems that can do this?
- Does your company want to run or lead the way in this topic area? (Tool-supported monitoring, Big Data, AI, etc.)

Possible approach to designing a system for early crisis detection:

- In-depth analysis of your company or business model
- Gathering and evaluation of information
- Definition of suitable early warning indicators in the form of key figures
- Subdivision into quantitative and qualitative indicators (exemplary)
- Creation and implementation of a suitable process / expansion of an existing process (e.g. use of the crisis management organization)
- Analysis and, if necessary, extension of the interface management
- Connection to existing reporting channels / creation of meaningful escalation levels and reporting channels
- Evaluation and, if necessary, expansion of your method pool
- Evaluation and, if necessary, integration of tools and systems
- Evaluation and use of meaningful external information (see chapter "Governmental and economic developments")
- Awareness raising

Summary

Management and executives have always based their decisions on concise data, presented at best in the form of key figures. This also applies to the prevention or at least containment of negative developments. Established departments provide suitable evaluations for this purpose, which often reflect negative developments in their own area of responsibility in a suitable manner. This contribution mostly relates to the collection of economic key figures and is thus closely linked to the monetary developments of the company. This also applies to thematically related areas such as risk management or controlling, whose financial and operational horizons can be further expanded by the ECD.

In addition to these key figures, regional, political and other less "tangible" framework conditions can also be considered to identify upcoming disruptions, emergencies or even crises. Frameworks that sometimes indicate huge damaging events (e.g., terrorist attacks, political unrest/attacks, epidemics/pandemics) but are disregarded or not even considered due to their lack of resilience. This also includes the constructive use or further development of the corporate culture, in which each individual employee responsibly and appropriately addresses information with suitable contacts and, in specific cases, escalates it.

However, current and future trends, many of which deal with the collection and processing of large amounts of data (Big Data) and the automatic detection of threats (AI), give rise to the idea that these worst-case scenarios in particular should be incorporated into companies' ECD. The activities shown in the environment of the federal ministries indicate that corresponding insights have already been gained politically. The use of corresponding developments could also be available to companies in the future and expand their prevention work. Regardless of government support, however, companies should take the legislature's higher requirements (StaRUG) as an opportunity to implement or adapt procedures for early crisis detection. This will protect your company from avoidable crisis events and make you even more resilient and fit for the future.

Controllit AG
Kühnehöfe 20
22761 Hamburg
Germany
www.controll-it.de

Status: October 2022

Controllit AG is your partner for Business Continuity Management (BCM). Since our foundation, we have been developing integrative concepts and products for business continuity management, IT service continuity management, Information security management and crisis management. We help you with strategic, organizational and technical concepts to secure your business processes against threats and to prepare for emergencies.