Crisis management

Whitepaper Working and practising with multiple incident teams

controllit
Business Continuity Management

Controllit is your partner for BCM, ITSCM, ISM and crisis management

Content

Introduction

A relay runner practices his run many times in the stadium before an upcoming competition, because practising in a professional environment is an essential part of securing results in his learning process. In the competition, the learned skills can be automatically called up in a similar environment and thus good results can be achieved. A relay team usually consists of four athletes who train on their own and meet from time to time to practise together. The athletes usually have individual abilities - one runs the curve well, the other the straight line. However, it is not only the individual performance of each member that is decisive for the result, but also the coordinated approach to handing over the baton. A moment in which valuable seconds can be gained or lost and which can decide the outcome of the race.

So what do a relay team and a company have in common?

Just as the relay team prepares for its competition, creates suitable framework conditions and practices procedures, a company can also prepare itself. In concrete terms, this means that employees are familiarised with situations and that a professional working environment and a suitable organisation are created. For both sides, it is essential to practice in order to be prepared for the competition or for the real event (from current topics such as cyber attacks, loss of supply media to the next pandemic, etc.) and to deliver good results.

Just like a relay team, which usually only wins the race if the individual runners perform well and the teamwork works well, it is the same in companies. On the one hand, the individual teams use their special knowledge and skills to advance their own team professionally, and on the other hand, they work together in a targeted manner to overcome the crisis.

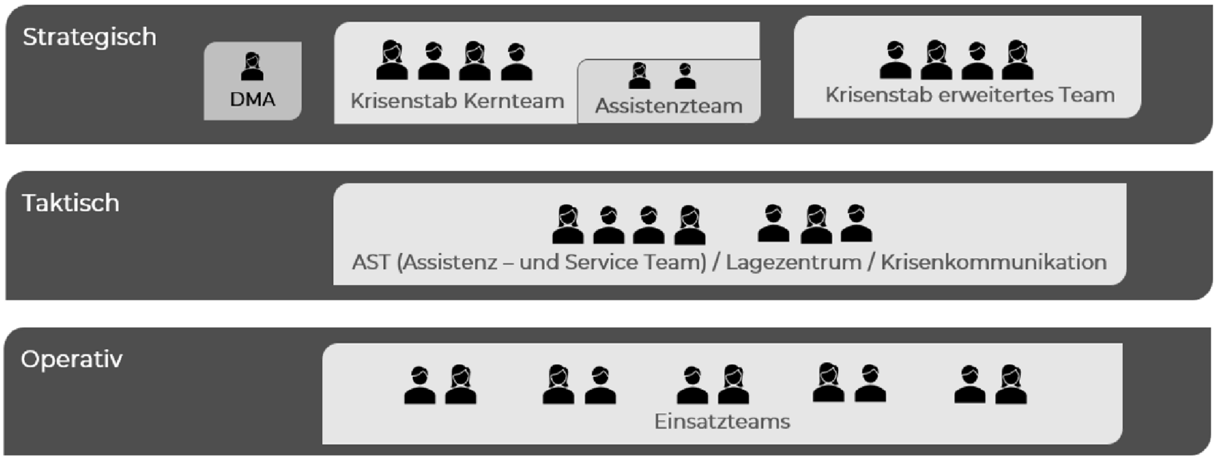
Introduction

Incident and crisis management organisations in companies are diversely structured and do not usually follow a single pattern. In deviation from the standard system, it may be that not four committees, but two, three or even possibly five committees (e.g. IT incident team, AST/situation centre, crisis management team) have to work together in an incident. In addition, companies often have to integrate external experts, contributors and staffs. Depending on the size of the company, the sector it belongs to and many other factors, there are different ways of organising it. Multiple teams in companies are therefore not uncommon and usually quite appropriate in order to bundle expert knowledge and to be able to deal with incidents quickly. We do not address the organisational forms of virtual, hybrid or face-to-face working here, as a diverse set-up is common practice in most companies today and has little influence on the good cooperation of multiple teams. You can achieve everything in all formats.

In this white paper, we show you how you can adapt your company well and equip it for acute crisis management.

Working with multiple teams: prerequisites and forms of organisation

The structure of a crisis organisation is classically depicted in three levels: strategic, tactical and operational, or gold, silver and bronze.



DMA = Decision Making Authority
Einsatzteams: BC-Teams, IT-Notfallteam, Evakuierungsteam, weitere Notfallteams etc.

- The crisis management team is located at the golden/strategic level (often also as a higher-level corporate or group crisis team), which makes strategic decisions, prioritises and carries out central information, measures and task management. The Decision Making Authority (DMA = corporate management) is the complementary body with overall responsibility for the company and provides support for decisions outside the mandate of the crisis management team or with an impact on areas outside crisis management.
- The Assistance and Service Team (AST), also known as the Situation Centre, forms the silver/tactical level, which supports both the strategic level and the operational level as a central point of contact and mainly takes on coordinating activities. In addition to the AST, there are other teams that can be deployed at this level: the crisis communication centre, the IT emergency team and/or the BCM coordination centre. In smaller companies, this function can also be performed directly by department heads, division heads or similar, who act as transforming control units.

Working with multiple teams: prerequisites and forms of organisation

As the interface between the strategic and operational levels, the AST is of great importance, as it is here that, among other things, communication and tasks are controlled, information is forwarded and processed in a way that is appropriate for the addressees, and, if necessary, evidence is also secured. and, if necessary, securing evidence..

- The actual acting response teams exist for each department and are assigned to the bronze/operational level. Their main task is to implement and execute the tasks at hand (with the support of BC plans, if available). They also follow the instructions decided and mandated by the strategic level and give feedback on the status and situation picture.

These three levels are organised in the established crisis management, a division of labour including roles and responsibilities is integrated and the connection down to the individual staff member is regulated. However, there are always practical challenges in the implementation regarding the powers of the individual teams.

Specific regulations and framework conditions for cooperation between the individual staffs promote targeted and coordinated cooperation. We recommend that, in addition to the lived practice, a corresponding anchoring in the documentation.

Crisis management teams in the company

Crisis organisations within companies are as individual and diverse as the companies themselves. In many companies, the classic structure of a crisis organisation is recognisable, but adapted to the size and orientation of the respective market.
So there are very different types of runners. In national companies with several locations, for example, this can mean that there is a crisis management team with several ASTs (one for each location) or even several crisis teams. A company with an international orientation will probably have several international crisis teams and its "own" AST and operational teams. A small company may not have any classic tactical teams at all, but rather the crisis management team, tactically acting departmental management and operationally reacting employees. If there are several strategic levels in a company (local/central crisis team and group/central crisis team), the need for regulation becomes obvious. However, the orientation of the teams is not only due to size or adaptation to the market. The respective event can also be decisive, especially if it concerns the (IT) technical or production side of the company. The baton must therefore be passed to the right place at the right time.

Superior, subordinate and external teams

A crisis organisation is primarily set up and convened in the event of a crisis in order to resolve it as quickly as possible and with as little damage as possible to the organisation and its employees. In order to make quick decisions, there are different hierarchical levels and correspondingly superior and subordinate teams.

Superior, subordinate and external teams

In the classic structure, the above-mentioned tactical staffs (AST, crisis communication, other situation centres, etc.) are to be regarded as subordinate teams to the crisis management team. In an international company, there is usually a corporate or group crisis management team to which other national and local crisis management teams can be subordinate.

But what does subordinate or superior actually mean? In order to steer the company out of a predicament in the event of an incident, a suitable structure must be found and the usually complex situation must be understood and managed. One of the highest priorities is the appropriate information management (including openness to errors, but with appropriate communication), the creation of a truly realistic overview of the situation and the organisation of decision templates until decisions are made.

Depending on the corporate structure (e.g. in the case of commercial and/or legal separation), this list can also have a legal component, where proactive regulation eliminates uncertainties in the event of an incident. Here again, many constructions are conceivable. A pragmatic solution for legally independent partners could be, for example, voluntary subordination. In any case, this should be legally examined on a company-specific basis and then established.

In addition, there are external teams that can be relevant and can only be influenced to a limited extent. If there is already a contractual and coordination relationship (e.g. with partners, suppliers, service providers), it makes sense to make binding regulations here. In the case of public authorities, this set-up is sometimes more difficult, but here, too, there has been a very positive trend in recent years, which a well-connected crisis manager can establish and expand through his external interface management. This in turn creates speed and procedural security in the event of an incident.

Superior, subordinate and external teams

The simplest **reactive means of implementation** are joint briefings/meetings of the different teams according to a clear organisational model, ideally based on the 3-level structure. But this also needs to be coordinated, planned, documented and implemented in advance with the potentially involved teams.

Shared Responsibility Model

A proactive means can be a shared responsibility model. Shared responsibility is literally translated as **common responsibility** or **shared responsibility** and describes with this contrast exactly the right scope: The common factor is the responsibility to lead the company out of the crisis in a cooperative and integrative way with all active teams. As a result, responsibility is shared at the different levels of the organisation and accordingly also in dealing with concrete tasks.

The Shared Responsibility Model provides the **proactive framework** for several teams working together constructively. Action and procedural security are described and assigned for the following parameters: Initialisation of team work, operationally secure information management, resilient execution of team-internal and joint briefings and, fundamentally, the delineation of the respective sphere of action. Furthermore, it promotes synchronous situation information, the processing of specific tasks, clear lines of command and a decision-making culture based on these.

The **aim** is to organise the various partners, local teams and bodies involved in managing a crisis in such a way that coordination, cooperation and communication are binding and uniform.

The Shared Responsibility Model can be used for the organisation of a central and decentralised system as well as for internal and external cooperation. The main goal is to develop binding lines of action for the respective teams.

Depending on the company's structure, a shared responsibility model works with a strategically active crisis management team and associated internal tactical teams, but also in more **complex company structures** with peer companies, several companies in different dependency formats, national and international subsidiaries (e.g. with a group/central crisis management team and further decentralised crisis management teams). In a shared responsibility model, external partners and service providers can also be reliably organised.

Shared Responsibility Model

The better and **more concrete the agreements and coordination in advance**, the faster and more targeted the crisis management activities can unfold. Here, too, it is important to make concrete agreements in advance, which should also be legally secured.

Overall, it is important for the concrete implementation in your company to identify the responsible persons, relevant partners, local/national/international teams and committees. Based on this, the company defines the principles and procedures for dealing with initial information and assessment, including escalation to the relevant teams.

Shared Responsibility Model

With a framework according to Shared Responsibility, a company **promotes the**

- the operational capability of each staff member (all staffs/all contributors),
- clarity on own tasks as well as the task context (delegation and escalation),
- speed and flexibility,
- consistency and direction according to the coping strategy, and
- Reliability including internal and external impact.

Information gaps, going it alone, apportioning blame, avoiding taking responsibility and empty promises are to be systematically avoided and significantly reduced in practice.

In addition to the above **preliminary considerations and factors**, we recommend a clear reference for all teams on how to proceed together, which can be based on the following idea-giving list specific to the company:

- Briefing organisation
- Facility Management
- Human Resources Management
- IT organisation
- Resource management
- Media support and external communication
- Customer care
- Service provider management
- Connection to authorities
- Welfare
- etc.

For this purpose, the following **parameters** should be assigned (e.g. by means of a legend):

- Responsibility/Leadership
- Participation/Support
- Joint commitment
- Readiness

The RACI matrix or a classic table format has proven to be a clear presentation.

Normative requirements/regulation

The various national, European and international regulations, standards and ISO standards contain as a common basis that there are escalation possibilities (via the known definitions and procedures on disruption, critical incident/emergency up to crisis) and a correspondingly structured cooperation of different organisational units that are to be tested and practised in order to secure plans and procedures. The depth of detail varies depending on the standard/norm and is now very extensive for regulated companies (keywords NIS/KRITIS, BAFIN or other supervisory authorities).

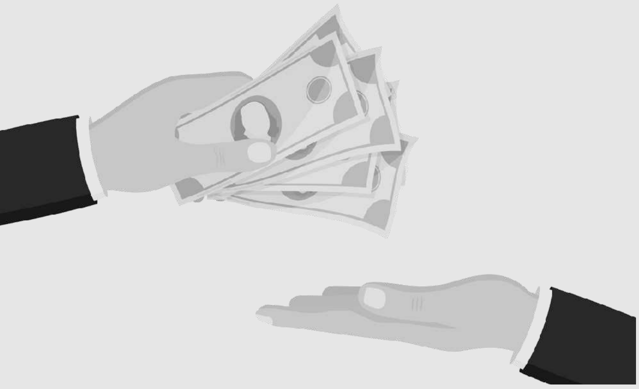
In a nutshell: The decisive factor for the design of the organisation and its validation (frequency and organisation of tests and exercises) is the industry affiliation.

Companies that are subject to regulatory supervision must demonstrate regular reviews of their emergency and crisis organisation in terms of effectiveness and adequacy. In addition, these companies must demonstrate that the validation follows a more demanding level of maturity.

Normative requirements/regulation

Some industry specifications even require full-scale exercises to be carried out on a regular basis (this is required, for example, in ITSCM with a data centre shift; in aviation and for airports, full-scale exercises are mandatory every 2 years).

A specific example:



If, for example, your company belongs to the **banking and financial services industry**, BaFin and MaRisk provide the holistic framework for the management of all material risks and thus also the regularity for reviewing the emergency[1] concept. Accordingly, companies belonging to the sector are obliged to review time-critical processes and activities at least once a year or on an ad hoc basis to test for all relevant scenarios . BaFin[2] requires different types of verification:

- Test of technical precautionary measures
- Communication, crisis team and alerting exercises
- Live or full-scale exercises

The MaRisk does not currently specify a specific timeframe for the concrete sequence/regularity.

Common to most of the regulations is that the scope of the inspections should always be based on the risk situation and that service providers should be appropriately involved. The organisation described above and the test formats with multiple staffs illustrated below are suitable for compliance.

1 According to BaFin, the contingency plan must include business continuation and recovery plans.
2 See Minimum Requirements for Risk Management - MaRisk, page 41

Test and practice with multiple incident teams

Tests and exercises help every company to assess how fast and resilient their organisation and functions are. Through tests and exercises, employees gain confidence in their actions and know what works, where the concrete performance lies and what can still run better.

Tests and exercises come in different levels of difficulty. Depending on the experience and maturity level of the teams, the tests/exercises differ in scope, the number of people involved, the scenario, the number of test objects and the depth of the test. First, a basic assurance is made and then there is a step-by-step increase in the scope, content and maturity level.

The following test and exercise classes are common according to best practice:

- Initially, **desktop or walkthrough tests** are usually carried out. Among other things, this test format identifies logical breaks and checks the completeness of the documents and their feasibility. Desktop or walkthrough tests serve as a plausibility check after an initial implementation. This test format is hardly suitable for multiple teams, but it is advisable to involve nominated members of the defined response team. However, it is advisable to involve nominated members of the defined response team.

- **Alerting tests** are carried out regularly for all relevant teams. In this test format, the accessibility, up-to-dateness of the contact data of the team members as well as the response time of the team are tested. This test format is naturally suitable for individual testing of the teams as well as for multiple teams. as well as for multiple teams. Since it is a very manageable test format test format, it will not be discussed below.

- In business continuity management and also for test objects of the crisis organisation, structures are checked via **functional testing**. This involves a practical and actual check of the conditions and processes as well as the technical facilities (procedures, availabilities and performance characteristics, availability of the required resources and work equipment as well as the interaction of the teams). This test format is already suitable for multiple teams, especially as an introduction to joint testing and practice. It is recommended to include selected functions from the different levels.

Test and practice with multiple incident teams

- The **simulation exercise** is an original test format of crisis management. Based on a concrete scenario, the functional capability is always tested with the aim of improving the skills of the exercise participants. This test format is very suitable for exercising multiple teams together. Depending on the level of maturity, the scope and the degree of difficulty can be varied.

- A **full-scale exercise** is a scenario-based real-time exercise to test the functionality and interaction of several stakeholders (teams, committees, functionaries, etc.) with the implementation of actual activities and, if necessary, the involvement of external forces (fire brigade, etc.) to test the coordinated interaction of the procedures. The test format "full-scale exercise" naturally involves a wide variety of stakeholders. stakeholders are involved, which is why it is also suitable for joint exercises.

Test objects can be documents (crisis organisation manual, crisis response plan, crisis communication plan, but also BCM manual and plans, etc.), but also working tools such as an alerting tool or the telephone chain, checklists, room equipment (virtual-hybrid and in presence), contact lists, virtual video conferencing tools, etc.

We recommend opening up the test planning for interdepartmental tests and exercises and integrating multiple staff exercises. In this way, synergy effects can be used in particular and resources can be planned in a target-oriented, sparing and further developing manner. Test planning coordinated with the management provides adequate support for implementation, also with regard to budgeting and risk assessment.

Test and practice with multiple incident teams

For all test formats where risks to regular business operations may arise, we recommend the creation of a test concept that should address the following points:

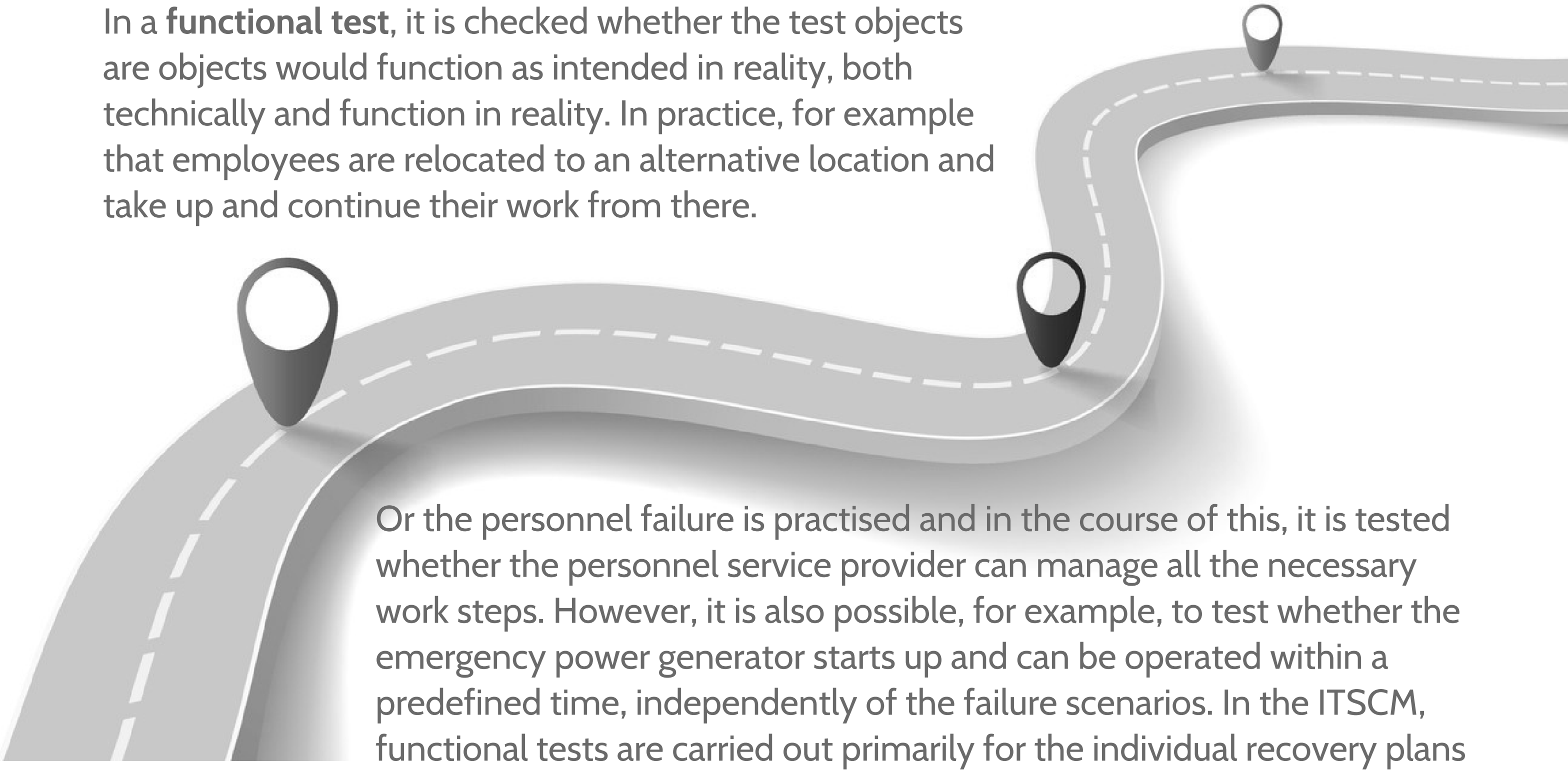
- Test/exercise objectives
- Time frame
- Methodology/format
- Use of resources incl. participants
- Prerequisites and characteristics
- Risk assessment
- Process planning

When creating them, an interdisciplinary interface exchange is usually reasonable.

In the following chapters we will go into more detail about the options and implementation possibilities of the individual suitable test classes for multiple teams.

Function tests

In a **functional test**, it is checked whether the test objects are objects would function as intended in reality, both technically and function in reality. In practice, for example that employees are relocated to an alternative location and take up and continue their work from there.



Or the personnel failure is practised and in the course of this, it is tested whether the personnel service provider can manage all the necessary work steps. However, it is also possible, for example, to test whether the emergency power generator starts up and can be operated within a predefined time, independently of the failure scenarios. In the ITSCM, functional tests are carried out primarily for the individual recovery plans and recovery plans for individual or bundled IT services. **Crisis management** checks, for example, the availability and application security of the working tools in the team as well as the practical applicability and coordination of the checklists and templates. In a functional test, it is not crucial to carry out the entire respective emergency management process, but the focus should be on checking the key figures.

Since a functional test can vary greatly in **scope**, this is already the first test class in which several teams can be included. You can extend the functional test to several teams or integrate individual key departments or parts of the company. The least time-consuming, but already very meaningful, is the selective integration of individual contributors from other departments. This can be a specific employee or a contact person at the service provider. They can participate in the test either as active participants or as observers.

These parameters can be used to control and limit the **planning and implementation effort**. With very little effort, the perspective of the test participants can be opened up to work in the environment of multiple teams.

Function tests

In any case, we recommend sharing the findings of the functional test with the respective neighbouring disciplines (i.e. within BCM, ITSCM and crisis management). From this, procedural security and reliability and also concrete implementation options can be derived.

Scenario exercises

While a functional test focuses on functional capability and tends to test professional and technical procedures, a scenario exercise focuses on qualitative characteristics in addition to quantitative ones. For this purpose, realistic stress situations are created in order to challenge and promote the crisis management organisation (all participating teams). The range of possible scenarios is vast. Ideally, a relevant and appealing topic is chosen in order to increase the motivation and participation of the participants on the one hand and to gain concrete professional insights on the other. In the current year 2023, the topics of hacker attacks, electricity and gas shortages as well as variants of supply chain bottlenecks are very much in demand.

If a company has already successfully conducted several scenario exercises with all the necessary teams, practising with several teams is recommended. Of course, this means a potentially higher central implementation and planning effort, but it saves on multiple individual planning. On the exercise day, a lot of resources and capacities are also tied up, but this is also more of a concentration than an expansion, as the individual teams would also have to exercise. However, a sufficient number of observers should be scheduled for the exercise day to observe and subsequently evaluate the actions of the individual teams. At least one observer with expertise should be planned for each team. It is advisable to have both internal and external observers to get a full impression.

Scenario exercises

A scenario exercise with multiple teams does not differ significantly from a scenario exercise with one team. In this test format, too, the **scope** can be controlled in a company-specific manner. From an exercise with one or two internal teams to the selective integration of an external crisis team representative to the integration of all scenario-relevant teams, a great deal is possible. If you cannot or do not want to integrate all relevant teams immediately, the inactive teams are simulated, as in the classic scenario exercise. Here, too, you can increase the realism by integrating a specialist staff contact person into your directorial team.

Scheduling will be a major challenge for a multiple team exercise and is likely to require considerable lead time (about six months in our experience). Therefore, it should be started quickly after the publication of the test planning.

Each scenario exercise should be **carefully evaluated and followed up** in order to further optimise crisis management structures and procedures. A report is recommended for this purpose, which should contain both positive findings and suggestions for improvement. Lessons learned and recommendations for action should be promptly communicated to all participating teams and addressed so that they can be used in a real scenario. It is advisable to draw up an **action plan**, assign the measures it contains to responsible persons and set deadlines for implementation. If there have not yet been any joint control dates, it is advantageous to include these as measures. As a rule, quarterly to half-yearly meetings are recommended.

The test class "Scenario exercise" is suitable both for the beginning of a joint practice as well as for advanced teams, because this type of exercise allows a lot of flexibility. In addition, this test class makes it possible to practise in a very sustainable way. Practising together usually has a high benefit for all staffs and accordingly also for the whole organisation. Working together in multiple teams not only promotes working with each other, but also enables each team to learn from each other (also professionally and structurally) - be it the taking of minutes, the approach to evaluating information or the contents of a situation meeting.

Another advantage of practising together is that it promotes understanding of roles, working methods and responsibilities across staff. This makes it possible to remain calm in a complex situation and to manage the event in a structured way.

Full-scale exercise

A company reaches the **highest level of maturity** when a full-scale exercise or complete simulation is carried out at regular intervals (approx. every two to five years - taking into account customary industry standards). This involves extensive practical involvement of the organisation and, if necessary, third parties such as service providers, the police or fire brigade. In a full-scale exercise, all prevailing plans (e.g. crisis communication plan, evacuation plan, BC plans and IT recovery plans) are applied in their entirety.

This test class is particularly suitable for practising **multiple teams** in a **realistic environment**. This test class uses the same procedure as the scenario exercise (planning, preparation, execution, follow-up). The clear advantage of a full-scale exercise (e.g. an RZ swing) is that it almost corresponds to a real scenario and the execution is carried out under "real" conditions. However, it must be noted that this test class thereby also sometimes involves high risks and can possibly trigger a real scenario. In addition, many resources are tied up centrally, especially on the day of the exercise and in the preparation. Here, an additional effort probably results not only from the coordination of the various teams, but also in particular with regard to bundling and coordination in advance.

A **full-scale exercise** should definitely be the goal of an advanced crisis organisation, but with due consideration of the risks and effort involved. Therefore, it is advisable to conduct a full-scale exercise with multiple teams only after functional tests and simulation exercises have already been successfully carried out several times.

For the **follow-up and lessons learned process**, the same procedure as for the scenario exercise can be used. However, due to the high complexity, we recommend dividing the exercise into implementation groups close to the staff after a central report and coordination of measures.

Outlook and conclusion

Our experience shows that the basic structures according to the crisis management organisation on the three levels (strategic - tactical - operational) are quite well established. So far, joint practice has tended to be treated carelessly by many companies. "**Too much money, too much effort, too much commitment of personnel**" are the most common arguments. This leaves it unclear whether the practical challenges described in the text, such as information gaps, going it alone, assigning blame, avoiding the assumption of responsibilities and empty promises, can be ruled out. An extended system on the working and framework conditions of several teams, e.g. according to the Shared Responsibility Model, is advisable and should also be tried out, i.e. tested and practised.

There is now a discernible trend for more and more companies to exercise their different teams together instead of separately. A trend that makes perfect sense, because the reality is indeed the same. An incident does not stop at different levels, but has to be solved together with the expert knowledge of each individual. The fastest individual runner simply does not win a relay race. Perhaps the experience of Covid-19 and the resulting increased maturity of many crisis management teams also support this trend.

We would like to take this opportunity to encourage you to expand your organisation and to practise with multiple teams.

Exercising with multiple teams can be very varied and individualised, both in the composition of the teams and in the scope of the exercise as well as the difficulty requirements.

In order not to overwhelm the teams, it is advisable to start with an announced joint scenario exercise, the handling of which is clear. If the exercise is successful, the scope can be increased. In perspective, the full-scale exercise should be included in the test planning, as it is most similar to a real scenario.

Outlook and conclusion

When practising together, it is not necessary to do this annually. As a rule, every two, usually every three years is sufficient for most companies. What should not be ignored are regular meetings between the teams.

In conclusion, preparation and practice are still the best training parameters. A crisis requires routine and structured procedures in order to cope with complex situations. To avoid siloed management, a coordinating structure and joint exercises are useful.

Open up your company's perspective on how to deal with multiple teams. Simply because the effort is quite small in contrast to the benefit and can make all the difference in a crisis for your company.

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

Status: September 2023

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, organisational and technical concepts to secure your business processes against threats and to prepare for emergencies.