Tooling for optimal resilience

Received (in revised form): 2nd January, 2020

Gert Kogenhop

Founder, bcm+, The Netherlands

Gert Kogenhop

Gert Kogenhop *is founder of bcm+, the business continuity management (BCM) consultancy firm. He chairs the Netherlands Normalization Institute's ISO Business Continuity Management and Crisis Management Mirror Committee and is an Honorary Member of the Business Continuity Institute. Gert has written numerous publications about business continuity and edits the BCM column for a regional magazine on sustainability. He is also Course Governor Resilience Management at the Security and Continuity (SECO) Institute in the Netherlands.*

ABSTRACT

This paper discusses the benefits of tooling as an enabler for resilience management, specifically business resilience. Business resilience entails the integration of different areas of expertise in a joint effort to secure the future of an organisation in a dynamic environment. It requires the right balance of risk management, information security and data protection, business continuity management and crisis management. To ensure that each area of expertise can operate independently within a coordinated framework, the right structure is essential. Much like a carpenter needs a hammer, the business resilience manager requires the right tools. Attention must be paid to collaboration, information sharing and balancing the right level of integration. While the tooling process will not be a panacea for the various challenges facing the business resilience manager, it will, however, be an enabler: it is beneficial, has deliverables and supports management and control.

Keywords: business resilience, tooling, collaboration, information sharing, integration

bcm+, John Raedeckerhof 29, 1628 ZA Hoorn, The Netherlands
Tel +31 229264797;
E-mail: gk@bcmplus.nl

Journal of Business Continuity & Emergency Planning
Vol. 13, No. 4, pp. 352–361

1749–9216

INTRODUCTION

Many organisations that have implemented a risk, crisis or business continuity management system do so by creating lots of Word and Excel files, supported in many cases by databases, and using PowerPoint or other office software to support the information flow. In some cases, SharePoint is used to make the system more robust and to create a secure environment for storing documents, calculations and other data components. Some larger organisations have built their own system or tool to fulfil their specific needs, but in most cases, these tools are difficult to maintain, let alone develop further in an ever-changing environment with evolving rules, regulations, requirements and demands. Organisations must ask themselves whether they have created a resilient management system that is ready to be used when required, or whether they have simply found the easiest way to meet the requirements of a document management system.

Every organisation is exposed to risks. Many are generic, like IT outage, building fire, utility issues or extreme weather; others are specific, resulting in a risk set particular to the line of business, be that chemical production, software development, construction, data management or baking bread. Location also has an impact on risk; for example, risks will differ between organisations located close to an airport, major waterway, chemical plant or oil distribution facility. Risk management, both enterprise and operational, is a must for organisations and, generally

speaking, it is reasonably well managed, especially in larger organisations where the use of integrated risk management tooling is common practice. This approach consists of a set of practices and processes to support and improve decision making and performance. It delivers an integrated view of how well an organisation manages its specific risk set. The world — especially the business world — is changing at a rapid and accelerating pace, so it is essential to keep one's eye on the ball when it comes to major issues such as climate change, Brexit and the so-called 'trade war' between the USA and China.

In today's world where everyone depends on information technology, information security and data protection are important elements that demand attention. In this regard, the European Union (EU) directive 'Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union'[1] and the General Data Protection Regulation[2] (GDPR) are important drivers. IT dependency makes organisations vulnerable and as such must be addressed and managed. Indeed, an IT outage can result in anything from a major disruption to the collapse of an organisation — something that would have been almost unheard of 40 years ago.

It is far too easy for serious disruption to develop into crisis. For this reason, crisis management and business continuity management are the prerequisites of a well-run organisation; indeed, in some countries they are even legal requirements. Being unprepared is simply unacceptable, and any 'plan' to act 'when the time comes' is not just poor business practice, but frankly irresponsible and unworkable.

BUSINESS RESILIENCE

Organisations must be stable and robust, and at the same time, resilient and agile. The term 'organisational resilience' has recently come to prominence, although there still is no agreement on how to define it. In itself, this is not an issue. The important thing is that organisations are prepared to invest time and effort in their overall goals, are aware that things can and will change, and are prepared to respond.

The two most commonly used definitions of organisational resilience are as follows:

- *International Organization for Standardization — Organizational Resilience (ISO 22316:2017)*: 'The ability of an organisation to absorb and adapt in a changing environment'.
- *British Standards Institution — Organisational Resilience (BS 65000:2014)*: 'The ability of an organisation to anticipate, prepare for, respond and adapt to incremental change and sudden disruptions in order to survive and prosper'.

At the SECO Institute, a group of specialists from different areas of expertise related to organisational resilience came up with a definition of business resilience based on the BS 65000:2014 standard. This definition is applicable for all organisations, whatever they do, wherever they are based, and combines the five previously discussed areas of risk management (RM), information security and data protection (IS/DP), business continuity management (BCM) and crisis management (CM) under the single umbrella of business resilience:

> 'The ability of an organisation to anticipate, prepare for, detect, respond and adapt to substantial change and sudden disruptions in order to survive and prosper by integrating management systems that build resilience, and develop capabilities for an effective risk response that safeguards the interests of key interested parties and restores the organisation's capabilities'.[3]

This definition is key for building a resilient organisation, whatever its goals and objectives may be. The SECO Institute definition builds on the British Standards definition through the addition of the how and why elements, as well as the word 'detect', as this is a must for people working in data protection. The word 'substantial' was also perceived to be a better fit than 'incremental'.

The main reasons for combining these five areas of expertise are:

- These combined areas already have the common goal of protecting the organisation's assets and securing the future;
- Linking the efforts is a matter of consistency and coordination through alignment, with numerous opportunities for synergy;
- The professionals working in these five areas of expertise will be far more effective and efficient, while still able to work independently and maintain their impartiality.

RESILIENT ORGANISATION

As discussed, some elements of business resilience will be specific to the organisation's particular line of business. In banking, for example, there will be elements related to licensing and supervision (eg EU regulation, Basel Accords or local national bank rules and regulations); in the food industry, there are quality and safety schemes (eg the British Retail Consortium Global Standard for Food Safety, International Featured Standards for the food sector and ISO 22000) and measures to combat product counterfeiting; and in the chemical industry there are many local requirements, such as those stipulated by the US Occupational Safety and Health Administration. In terms of risk management, two important elements to have emerged as a result of the Sarbanes-Oxley Act 2002 are governance and compliance. These also need to be factored when applicable. Where these elements are a consideration, governance risk compliance tooling is commonly used to ensure capabilities are optimally integrated to achieve objectives, address uncertainty and act with integrity.

From this perspective, business resilience can be described as a 'joint crisis fighter' — a bit like the F-35 'Joint Strike Fighter', which can collect and share more data in a short period of time than any other aircraft. Obviously, one must be careful with comparisons, but sharing and collecting information is at the heart of a resilient organisation.

COLLABORATION, INFORMATION SHARING AND INTEGRATION

Collecting and sharing information during any disruption affecting the delivery of prioritised products and services, such as a cyber incident, collaboration between the crisis management team (CMT), the cyber security incident response team (CSIRT) and the business continuity management team (BCMT) is of the utmost importance. Clause 8.3.4 of the ISO 22301:2019 Business Continuity Management Systems — Requirements standard includes a list of the resources that need to be determined before implementing selected strategies. Slightly tweaked, these are:

- People;
- Information and data;
- Physical infrastructure such as buildings, work spaces or other facilities and associated utilities;
- Equipment and consumables;
- Information and communication technology (ICT) systems;
- Transportation;
- Finance; and
- Partners and suppliers.

In the case of a cyber incident, there are specific elements that also need attention. These are:

- Security of (personal) information/data;
- Rules and regulations;
- Brand and reputation; and
- Communication with stakeholders and media.

When mapping these over the three teams involved in a cyber incident, it is clear that certain elements and resources are team-specific. For example, brand and reputation and communication with stakeholders and media should be managed by the CMT; security of (personal) information/data should be managed by the CSIRT; and resource-related activities regarding physical infrastructure such as buildings, work spaces or other facilities and associated utilities, as well as equipment, consumables and transportation should be managed by the BCMT. Again, the various teams should be able to work independently and maintain their impartiality. Nevertheless, when it comes to the other resources, specifically the element of rules and regulations, this will in most instances require the involvement of all teams, even if they have different goals. For the CMT, for example, information regarding the cyber incident will be of the utmost importance in order to determine the severity level and what to communicate to whom, all while taking into account the applicable rules and regulations. For the CSIRT, information is a requirement for the process of detecting and responding. The BCMT needs information to assess the situation and execute the appropriate scenario(s) in order to continue delivery of products and/or services at acceptable predefined levels. To interpret all this intelligence, however, requires a coordinated team effort; for this reason, a shared command centre is a prerequisite for a successful response. Collaboration, information sharing and integration are concurrently both key words and challenges (Figure 1).

BUSINESS RESILIENCE MANAGEMENT SYSTEM

To secure resilience, every organisation should appoint a specific individual to

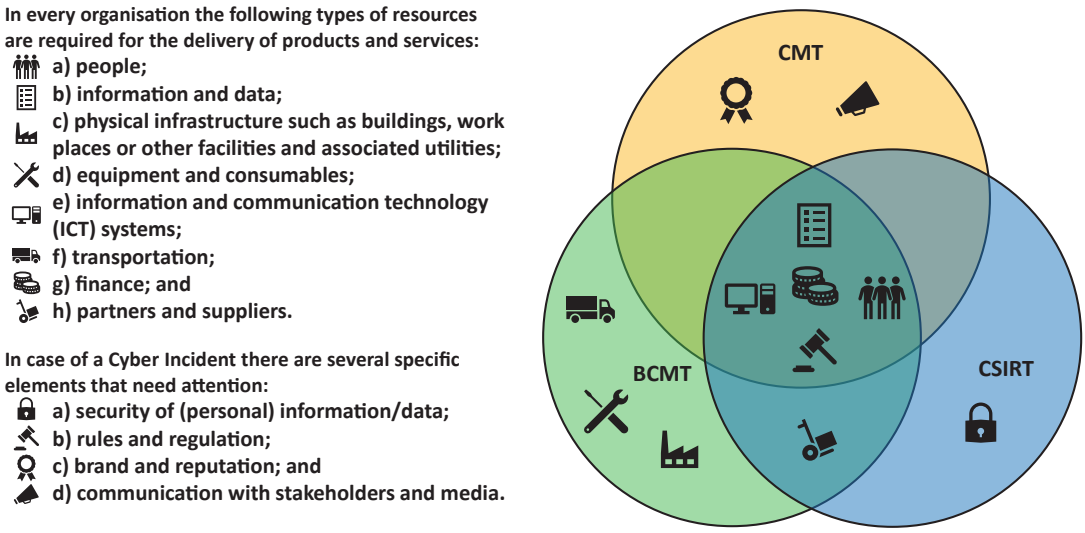

Figure 1 Cyber incident — Collaboration, information sharing and integration

manage its business resilience effort. To ensure successful implementation and execution, the owner of the business resilience process must be able to report directly to the C-suite.

When it comes to business resilience, many organisations are still in the development stages and only a few have established a management system. Maturity levels remain low and, for many, a statement like 'business resilience is embedded in the way we work here' would seem a bridge too far. Business resilience is still a relatively young area of expertise and organisations are looking for support and best practices to improve their efforts. Implementing business resilience management and creating a management system in any organisation with siloed expertise is challenging. After it has been concluded that the organisation needs to implement a business resilience management system and that for this it requires a business resilience manager, the challenges become much more specific. There will be well-established silos of resilience activities, often isolated from technology and the supply chain. The current information will probably be buried in Word, Excel, SharePoint and assorted homemade tools. Most processes will be manual, inefficient, resource-intensive and take too long to execute. The total effort 'lags' behind the organisation and cross-organisation reporting capability is limited. The situation is likely to be ambiguous, inconsistent, inaccurate and not create any value as a whole; as a result, there is limited opportunity to repurpose. This is inefficient and must be addressed by the business resilience manager.

For the business resilience manager, one of the biggest challenges relates to aligning the cultural side of business resilience. The different areas of expertise will be used to working on their own, in isolation, albeit in line with the organisation's mission, vision and strategy. Risk management is the common field of expertise that the various areas will be familiar with, but all will have different goals. In addition, crisis management is a 'separate' specialised, mostly centralised process that is used only in the event of an incident that requires invocation of the crisis management plan and installation of the crisis management team. The level of embeddedness differs from both business continuity management and information security and data protection. Business continuity management is partially embedded; it is the combination of preparing for and acting/reacting when an incident occurs and invocation of the business continuity plan is required. Information security and data protection are fully embedded in the organisation and its day-to-day operations. While all this may affect the governance approach, all should be aligned and there should be no organisational islands. What all areas have in common is the need to focus on vision, purpose and awareness. For the business resilience manager, strong leadership is a prerequisite for success to be embedded. From a cultural perspective, crisis management is about communication and collaboration. Responding to a crisis requires information to be shared across all parts of the organisation. A specific business continuity management focus is around commitment and ownership — process owners need to be driving the execution of their recovery activities and they need total commitment from all involved in the organisation, starting with top management. Here as well, information sharing and collaboration are key success factors. The fully embedded information security and data protection effort focuses on securing the right behaviour and discipline from all system users. Information sharing and collaboration with all stakeholders is of the essence (Figure 2).

Figure 2 Business resilience management and culture

TOOLING

Tooling is not the solution for all challenges facing the business resilience manager. It will, however, be an enabler: it is beneficial, has deliverables and it supports management and control, with particular regard to the previously discussed areas of information sharing and collaboration. Integration is the only way to secure control and avoid any surprises as a result of activities (or lack of them) from separate silos or organisational islands.

Based on the need to optimise the business resilience effort, tooling must consider the specific needs of the various areas and address:

- Risk assessments (from different angles);
- Crisis management plans (eg per country, site, central and strategic);
- Business continuity plans (eg process, product or activity level);
- Disaster recovery plans (eg resource plans, equipment, applications, network); and
- Cyber attack response plans (eg hacking, ransomware and data breach).

At the same time, more specific plans can be added if and when required, all using the same template structure but customised for specific needs and requirements. A single access point is a requirement, and the options for setting user profiles should be adjustable in line with the organisation's governance policy.

The use of software enables the underpinning of a solid business resilience practice. From an intellectual point of view, it enforces both the mandatory and optional elements of policy compliance and process management, all recorded in the appropriate way. From an organisational perspective, it reflects ownership and the approval process at the right level, by assigning owners for all elements of the tool, such as the business impact analyses, risk assessments and plans, while establishing roles and responsibilities for all involved by tight governance

management, including strict user profiling. From a system management point of view, it enables rapid change management. Tooling facilitates robust change management across multiple documents, saving time while ensuring consistency and accuracy. From a logistics point of view, there will be a single repository. As a result, there should be no inconsistency in data import and output, as well as the ability to manage large volumes of data. Further, an automated workflow including optional e-mail messaging and internal service-level agreements regarding the creation, development, approval and maintenance of all segments in addition to the reporting of results should be included. Finally, from a cultural perspective it will drive the right behaviour as the use of templates will create constrain deviation to create a single way of working.

The use of software delivers grip, structure and drive. These elements are very important when managing business resilience. End-to-end process support is an important key for success, as are the ability to view administrative dashboards at different levels; produce executive dashboards with, for example, information on key performance indicators and status; and compliance dashboards focusing on policy or standard compliance status. This structure delivers the ability to produce risk assessment from various angles, such as by site, country or line of business. For business continuity management, this relates to the business impact analyses from different levels, such as strategic, tactical and operational, as well as by department, discipline or process. The most important deliverables are the business continuity plans that include the different scenarios required and address the outcome of the risk assessment. Plans are the most important deliverables for the crisis management effort as well, with specific needs regarding the assigned responsibilities concerning brand and reputation management and communication with stakeholders and the media. For information security and data protection, the ability to execute the required plans and execute the recovery activities flawlessly are the most important aspects that need to be delivered through tooling. Linked to the execution of plans is the need and, as a result, the ability to test and exercise. The right tooling should include emergency communication possibilities (notification) or at least the option to link to existing notification tooling. To fulfil one of the most important requirements of business resilience, tooling should deliver incident management the possibility to invoke all previously mentioned plans if and when required, along with the ability to have an overview and drill down to the execution level of a specific plan. This centralised overview results in less disruptive communications between teams and management while executing the required plan responses.

The benefits of the use of software are substantial. Software delivers consistency — a single way of working supported by the use of templates when conducting, for example, business impact analyses or risk assessments. The use of dropdown menus obviates the need for manual data entry, allowing for consistent descriptions while facilitating bulk entries. Templates are also useful for introducing resource sets (eg people, IT equipment, applications, office equipment) and other preset items, while maintaining a degree of flexibility and customisation. The resource sets should be built on and connected to 'golden source' enterprise data, like the human resource database and the configuration management database. Efficiency through the use of the automated workflow and the proactive and dynamic management of change plus exception management are very valuable. Central visibility regarding the status of the management system as well as the

actual situation during an incident or disruption is invaluable.

The added value of having a data set that is unique in any organisation and is underpinned by the connected data sets should not be underestimated. Having the ability to cut and slice data including resources like people, property, technology and suppliers adds value to the whole organisation, not just the business resilience department. Setting up the tooling hierarchy is one of the most important steps, as this defines the capability and ability to view and report on different levels of the operating structure and at the same time by geographical area when needed. If set up correctly, it should be possible to filter data, for instance, by business area, process, product, service and business line. This allows users and administrators to produce 'what if' analyses that focus on every aspect covered in the system. By running a 'what if' report focused on the application being unavailable, 'what if' reports can even support decisions regarding when to upgrade or replace an application. When the results show the dependency is high, this could lead to a different timing or way of upgrading. This same report can be used for prioritising information security and data protection efforts and investments. Another example is when moving departments from one building to another over the weekend. 'What if' it is not ready on Monday morning? What processes and products, for instance, will be affected? This can lead to a request (supported by the data) for more people to get involved in the actual move. Other possibilities include dependency reporting, both internal between departments and functions, as well as external with suppliers and business partners. This could lead to specific insights and, in cooperation with the sourcing/purchasing function within the organisation, mitigation of dependency, for instance, through the appointment of alternative suppliers, tackling the issue of single sourcing. The added value of this data set is substantial and when used properly will increase the overall organisational, operational and business resilience, whatever it is called or whatever the content in any specific situation may be.

Key messages from users of tooling can be summarised as follows:

- Thinking beyond the replacement of manual business impact analyses and plans;
- Reporting at the time of an incident, not just business as usual;
- Understanding the importance of a valuable data set;
- Opportunities for more up-to-date and dynamic data, ownership at the right (process) level;
- Easier workflow management and maintenance with less resources (cost savings);
- Consistency, conformity and clearer governance, with more insight into all aspects.

For this to be possible, tooling should:

- Be dynamic, flexible and evolving;
- Be accessible from different devices and locations;
- Be actionable, including tasks and actions with assignments and timing when required;
- Be intelligent, with the possibility of (scheduled) reporting and access to the data repository;
- Have the right level of confidentiality, integrity, availability and authenticity; and
- Have the option to be viewed from organisational or geographical angles, global or in detail.

To guarantee it is fit for purpose, tooling must be configurable. It should be user-friendly and guide users through all steps to

ensure optimal onboarding and use. Most organisations look at selection categories like ease of implementation, functionality for their needs and requirements, performance and support. Customer satisfaction scores should not be forgotten. Happy users are important for quality content and flawless execution when required.

CONCLUSION

The complexity of business resilience, management of change and ongoing development including the need for continuous improvement and the required speed of action, require the integration of all areas of expertise. Linking the efforts of all the aforementioned elements, specific to the situation, leads to consistency and coordination through alignment, with numerous opportunities for synergy. All involved will be far more effective and efficient, while still able to work independently and maintain their impartiality. The essential factors are collaboration, information sharing and integration, where and when applicable.

Tooling is essential for optimal resilience, whether it be organisational, operational or business resilience. It is an enabler, it is beneficial, has deliverables, and leads to optimal management and control. It will drive agility in decision making and build confidence when executing plans and procedures when required. The use of tooling shows a high level of professionalism and maturity around the implementation of resilience management and all its elements, and will undoubtedly build confidence with interested parties, especially regulators, owners and executive management, as well as partners and customers.

APPENDIX: THE USE OF SOFTWARE, STUDIES AND RESEARCH

Many consulting organisations, institutes and other specialists have produced white papers, studies and research regarding resilience, most notably organisational resilience. From a business continuity perspective, there are several initiatives, both new and well established, that provide a useful foundation for the assessment of resilience tooling.

In a recent business continuity benchmark study,[4] just over one-third of respondents reported 'still' using spreadsheets and text-based documents, while slightly fewer reported using commercial business continuity software. Among larger organisations (>1,000 employees), GDPR compliance appears to be a key motivator for the move away from standard office applications like Word and Excel. On average, one in nine large organisations uses custom-built software applications. For organisations of all sizes, the highest-ranked features of business continuity software are the ability to manage plans, business impact analyses, and continuity strategies, followed by features needed during a crisis. These were ranked 'critical' or 'important' by more than 50 per cent of respondent organisations and include the ability to map dependencies, contact employees and manage the crisis both locally and centrally.

Gartner[5] frequently produces research reports in this field. Its 'Magic Quadrant for Business Continuity Management Program Solution, Worldwide' is highly regarded and used by many organisations around the world. The report highlights leaders in the industry as well as challengers based on their assessment of completeness of vision and ability to execute. Also available from Gartner is a research document titled 'Critical Capabilities for Business Continuity Management Program Solutions, Worldwide'. As the title suggests, it focuses on the ability of providers to deliver the critical capabilities defined by users.[6]

CIR Magazine (www.cirmagazine.com) frequently issues three different software

reports to help select the best in class in specific areas. With respect to resilience, however, it should be noted that suppliers must *not only* be best in class with respect to expertise, but must *also* be able to deliver resilience capabilities. The business continuity, emergency and mass notification and risk software tools all give readers a market analysis and the possibility to compare different suppliers based on product features. The goal, however, should be to have a single tool. If this is not possible, make sure the selected tools are linked when required without jeopardising the benefits discussed previously.

References

(1) The European Parliament and the Council of the European Union (2016) 'Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union', available at: https://eur-lex.europa.eu/eli/dir/2016/1148/oj (accessed 31st January, 2020).

(2) The European Parliament and the Council of the European Union (2016) 'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)', available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj (accessed 31st January, 2020).

(3) Kogenhop, G., Bakker, J. and Kuethe, M. for the Security and Continuity Institute (2019) '2019/2020 Business Resilience Masterclass', available at: https://www.securityacademy.nl/opleidingen-overzicht/masterclasses/br-masterclass/ (accessed 31st January, 2020).

(4) ClearView and Assurance (2019) '2019 Business Continuity Benchmark Study', available at: https://www.clearview-continuity.com/content/media/archive/2019/17Sept2019.asp (accessed 31st January, 2020).

(5) Gartner Research (2019) 'Magic Quadrant for Business Continuity Management Program Solution, Worldwide', available at: https://www.gartner.com/en/documents/3957353 (accessed 31st January, 2020).

(6) Gartner Research (2019) 'Critical Capabilities for Business Continuity Management Program Solutions, Worldwide', available at: https://www.gartner.com/en/documents/3967984 (accessed 31st January, 2020).