Business Continuity vs Operational Resilience

Having just read the Operational Resilience Report 2022[1] from the BCI and partners Castellan, I feel compelled to question some of the conclusions.

It is clear that, with the emergence of 'resilience' as a concept, there is a lack of clarity in the differences between organisational resilience and business continuity, and the water has been further muddied by references to a new term, 'operational resilience'. This report could have presented an opportunity for some clarity and consistency, but in this short article, I propose that, instead, the report has created additional confusion and, in some cases, denigrated the expertise of business continuity professionals.

I will start with a short background in order to give some historical context based on my own experiences within the industry. I will then analyse some of the specific content and contradictions of the report, before highlighting my conclusions and concerns.

Personal Historical Context

I joined the Business Continuity Management (BCM) profession in 2001, initially as part of a local authority emergency planning role, before transferring into more BC focussed positions. I have therefore seen the transition and standardisation of the industry, from the early days of PAS 56[2], that glorious acronym-laden document that first gave a structure to Business Continuity (BC), to BS25999[3] and, more recently, to ISO 22301[4][5].

I have clear recollections of discussion and debate about raising the profile of BC, with many voicing concerns that the title of the profession was not very alluring or 'sexy', and that there was a failure to gain traction with senior management. Many expressed concern that BC would never become a 'c-suite' role, and endeavoured to expand the scope to ensure that more senior positions could be obtained. Moreover, those in the public and third sector were keen to point out that they did not do BC, but focussed more on 'service continuity'.

Gradually, the term 'resilience' became more of a feature in discussions, without ever being clearly defined within these discussions. BS25999 did broadly define resilience as 'ability of an organization to resist being affected by an incident'. An updated definition can be found in ISO 22300 [6]as 'ability to absorb and adapt in a changing environment'. As a side note, it is interesting to see the gradual change of category of standard, from 'societal security' to 'security and resilience'.

The many debates around the role of business continuity within an organisation led to some to call for a wider input into more general business resilience, such as reacting to market changes, and beyond those 'catastrophic' events that were generally considered for BC planning purposes. This, personally, always seemed a little beyond the scope of a business continuity role, and stepping into the role that would traditionally be covered by, for example, CFOs and COOs, the majority of whom I

[1] Operational Resilience Report 2022: BCI report
[2] PAS 56:2003 Guide to Business Continuity Management
[3] BS25999:2006 Business Continuity Management Part 1 Code of Practice and Part 2: Specification
[4] ISO 22301: 2012 Social Security – Business Continuity Management Systems - Requirements
[5] ISO 22301: 2019 Security and Resilience – Business Continuity Management Systems - Requirements
[6] ISO 22300: 2021 Security and Resilience - Vocabulary

could safely suggest would have a greater experience at dealing with, for example, swings in the markets. However, the concept of Organisational resilience' was formed and with it, naturally, another standard[7].

Organisational resilience has been defined within ISO 2016[7], and is clearly quite distinct from BCM. In this article, therefore, I do not propose to look at the content and context of organisational resilience. Instead, I intend more to look at what has appeared to become more prevalent terminology, without actually being defined…'Operational Resilience'. The use of the term appears to be largely led by the finance sector, in particular the Financial Conduct Authority (FCA) in the UK, and this is acknowledged in the BCI report[1]. However, as is recognised by the report, there is no agreed definition for this concept.

Have the BCI got it wrong?

The Executive Director of the Business Continuity Institute suggests in the report[1] that operational resilience is separate to business continuity, concluding that '*most commonly the Chief Operations Officer, is responsible for championing operational resilience programmes, the implementation and day-to-day management of operational resilience frequently falls on the shoulders of the Head of Business Continuity. This has inevitably led to some confusion; "operational resilience is just business continuity done well" was a sentence often repeated by respondents over the course of this project. As a result, this report seeks to define the very real difference between the two interlinked resilience methodologies*.' This blatant disregard for the experience of the BCI members is surprising.

If we break down some different aspects of the report's findings, this article will demonstrate that 'business continuity done well' is, indeed, effective operational resilience.

The report suggests that '*business continuity focuses around getting processes back up and running in an agreed timescale. Operational resilience centres around the principle of having to get a process up and running before it causes intolerable harm to the business, its customers or its peers*.' Perhaps the authors should consider the definition of BC within ISO 22301: 'capability of an organization to continue the delivery of products and services within acceptable time frames at predefined capacity during a disruption. Or, indeed, the definition within the BCI's own Good Practice Guide, which states that '*A holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities*.' Note that this makes specific mention of stakeholders, defined as '*person or organization that can affect, be affected by, or perceive itself to be affected by a decision or activity. EXAMPLE Customers, owners, personnel, providers, bankers, regulators, unions, partners or society that can include competitors or opposing pressure groups*', a definition which, I think, covers customers and peers, as well as others.

Fundamental to any BC programme is '*Understanding the needs and expectations of interested parties*', whereby an organisation needs to identify the interested parties that are relevant to the BCMS, and the relevant requirements of these interested parties. This is clearly demonstrated in ISO 22313, which depicts the relationship as:

[7] ISO 2016: 2017 Security and resilience — Organizational resilience — Principles and attributes

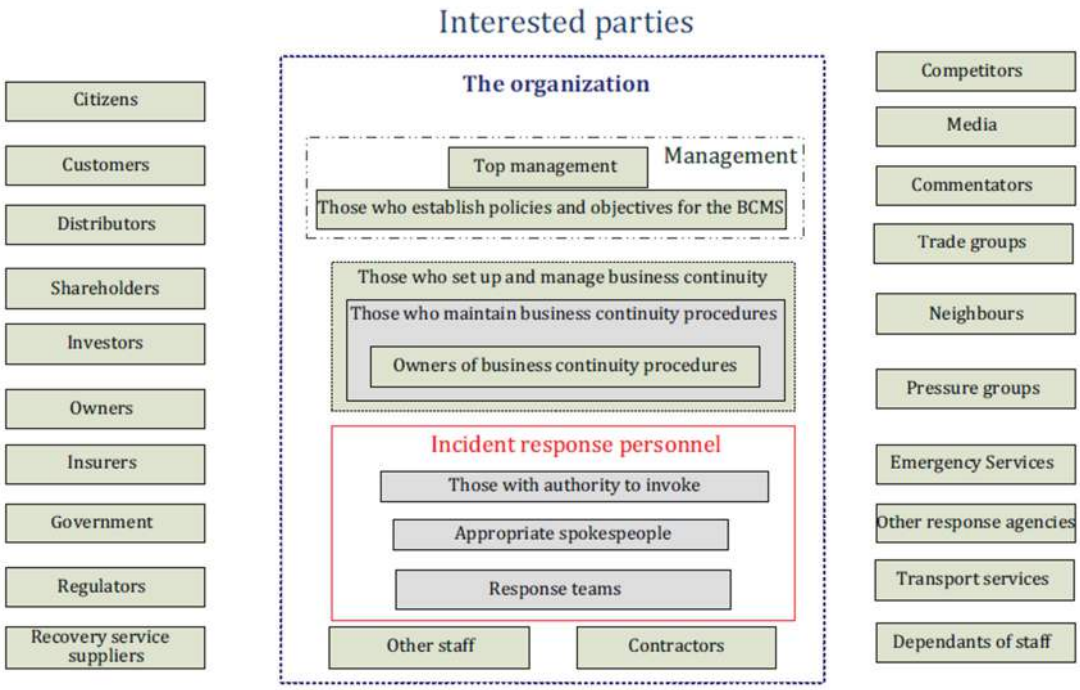

Figure 4 — Examples of interested parties to be considered in public and private sectors

Time and again, the standards and guidance documents make reference to stakeholder requirements and expectations, and the need for these to be taken into account.

The BCI report gives a quote from an Operational Resilience Consultant, who states that "*Business continuity is about how quickly you want to have a process back up and running, whereas operational resilience is how quickly must that service be back. And it's a different question*."

This shows staggering naivety, and it is very surprising that the BCI chooses to list this quotation within one of their own surveys. The report states that '*Some 17.1% of respondents believe there is no need for an operational resilience programme within their organization as "business continuity is all that they need." When you consider this rises to 25.0% when looking at responses from the financial sector alone, this is even more alarming. Indeed, the opinion that operational resilience is "business continuity done well" is one subscribed to by many resilience professionals*'. Perhaps the authors of the report should consider that these respondents are BC professionals who have a level of experience within their field.

I am not sure for what reason that BCI appear to be being led by the FCA as seems apparent throughout the report, but it is worth reflecting on some of my own experiences within the BC profession.

As far back as 2008, we illustrated the difference between disaster recovery and BC, showing the following slides to a client as part of a training session:

Here, it is clear that, almost 15 years ago, BC was focussed on customer interests. This same focus has been promulgated by BC practitioners time and again.

Another example could be the Business Impact Analysis involved looking at impacts on the customer, thus a BIA with a pharma client, for example, required our clients to revaluate their top 10 product list to develop one from a patient criticality perspective as well as from a profit perspective. Or the printing company that knows that it has clients who come under the Civil Contingencies Act 2004 and therefore have specific requirements around continuity of supply. Or the manufacturer of printers who split customers into different groups dependent on their specific time-critical supplies.

The consultant quoted earlier simply does not seem to understand that to know how quickly you want to have a process back up and running, you need to understand how soon your various stakeholders require that service or product.

Another aspect of the reports comments on staff awareness, highlighting *'interviewees reporting knowledge of operational resilience simply was not there in the organization. With operational resilience still a new concept however, even the experts in the field believe that this knowledge can only come once the regulators have learned themselves what best practice is'*. Given that there are relatively few regulated industries, it is difficult to see how there can be widespread awareness of operational resilience at this point particularly, as highlighted in the report, '*Operational resilience means different things to different sectors and also companies within the different sectors', and that there is no single definition of this concept*.

The BCI report suggests that '*the Board and, most commonly, The Chief Operations Officer is most likely to have overall accountability for operational resilience, although other board level members are responsible in some organizations', whilst 'Business continuity is most likely to take the day-to-day lead on operational resilience, particularly in organizations without a dedicated operational resilience team'*.

Taking aside the fact that most organisations simply will not have the resources or staff to have two teams working on identical work, the ISO 22301 requirements include top management demonstrating leadership and commitment, whilst being able to delegate roles, responsibilities and authorities. The BCI's own guidance[8] suggests 'assigning a member of top management overall

[8] BCI Good Practice Guidelines 2018 Edition

accountability for business continuity and its effectiveness', whilst allocating roles and responsibilities based on competency.

So where does this lead us?

Significant mention is made of the FCA approach to operational resilience and business continuity within the recent BCI report, with a surprising amount of deference to the FCA approach. Having worked with a start-up challenger bank, it is obvious that the guidelines and requirements are causing duplication of effort and, possibly, the creation of yet more siloed thinking. Despite demonstrating that an effective approach to business continuity completely mapped into the operational resilience requirements, the bank simply did not have the confidence to merge the approach, and insisted on maintaining a separate set of documentation to satisfy the requirements for Operational Resilience, thus creating needless duplication, and increased likelihood of errors, and a lack of joined up thinking leading, possibly, to a reduction in resilience.

It saddens me to see the BC professional institute adopting a BC vs Operational Resilience approach. Surely, they should be taking account of those practitioners who 'do BC well', and recognising that BC **is** operational resilience, just under another name. Possibly a 'sexier' name, and it certainly seems to have gained traction in some industries. However, I am sure that those practitioners who debated name changes all those years ago did not envisage that this could lead to a schism in the industry, and accusations that BC is basically an internally focussed and retrograde approach.