noggin

Business Continuity

Guide to Understanding ISO 22301: Management system requirements for Business Continuity

Moving toward a business continuity management system (BCMS)

As Business Continuity Management (BCM) practitioners know well, the business continuity plan (BCP), which helps ensure critical operations remain available and minimize business impacts, irrespective of the type of incident or disruption, is the cornerstone of any best-practice business continuity program. The BCP is absolutely essential to the business continuity manager's task of identifying, quantifying, and minimizing potential business interruptions and risks.

Here, the data is clear. Business closure numbers are heavily weighted towards companies that fail to develop BCPs before major incidents; in fact, as many as three in every four organizations without a business continuity plan fail within three years of a disaster[i].

As dispositive as those numbers are, there's still an element missing; for companies that have developed BCPs and disaster recovery plans aren't out of the woods quite yet. Having a BCP during the prevention and preparedness phases is one thing, but executing the plan promptly once a disaster has taken place is *the* key business survival factor. After all, companies that are unable to resume operations within 10 days of a disaster striking are unlikely to survive[ii]. Further, 80 percent of companies that do not recover from a disaster within one month are likely to go out of business[iii].

Companies that are unable to resume operations within **10** days of a disaster striking are unlikely to survive.

Further, **80**% of companies that do not recover from a disaster within **1** month are likely to go out of business.

That's why the best business continuity programs also develop business continuity management systems (BCMS), defined as the overall management system that establishes, implements, operates, monitors, reviews, maintains, and improves business continuity. Developing systems, rather than just plans, enables businesses to better understand needs and evaluate the necessity for establishing business continuity management policies and objectives. There is also growing evidence that organizations that have not implemented a Business Continuity Management system are more likely to fail after a major disruptive event[iv].

What's more, a BCMS reinforces the importance of implementing and operating controls and measures for managing an organization's overall capability to manage disruptive incidents. Taking a systems-approach also helps ensure continual improvements based on objective metrics. The question remains, though: how to build a best-practice BCMS?

Business continuity management: the essentials

Business continuity management (BCM) has been around for some time now, roughly since the 1970s. Emerging, then, as an offshoot of crisis management, BCM defined itself as the field dedicated to effectively responding to the technical and operational risks that threaten an organization's recovery from interruptions.

The scope has since narrowed. BCM today is a holistic management process for identifying potential threats to an organization and the operational impacts those threats pose. Nowadays, it's the primary task of business continuity professionals to build a durable framework for organizational resilience, in compliance with regulations and prevailing business standards like ISO 22301. This core responsibility brings business continuity professionals in close contact with other safety and security practitioners, including those in safety, risk management, disaster recovery, emergency response, and crisis management.

But the tools of business continuity management are fundamentally different, though. One mainstay is the business continuity plan (BCP), a collection of resources, actions, procedures, and information, designed to prepare organizations to maintain essential functions in the event of a disaster or other major disruption.

Sources: Brahim Herbane, Business History: The evolution of business continuity management: A historical review of practices and drivers.

A deep dive into ISO 22301:2012

One answer comes courtesy of the BCM standards on the market today. Those standards offer an extensive list of best practices to help organizations design their own business continuity management systems so as to achieve maximal outcomes. Chief among those standards is ISO (International Standard Organization) 22301:2012, the sole, high-level, international BCM standard, using recognized best practices. The international standard specifies requirements to plan, establish, implement, operate, monitor, review, maintain, and continually improve a documented management system to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise[v]. So even if businesses don't wish to achieve compliance with the standard itself, they can still enjoy the benefits of a well-implemented BCP system, namely organizational resilience.

A little history, first. When ISO 22301 first emerged, it superseded the British standard BS 25999. The national standard had only appeared a few years prior, in its place superseding the British specification, Publicly Available Specification 56 (PAS56).

BCM analysts note few differences between BS 25999 and ISO 22301. Both standards offer methodical, systematizing approaches to business continuity, operational resilience, and incident response.

By definition, though, ISO standards are management system standards; they also come with a specific format. That's why the principal distinctions between the British and international standard are those of format. It's been noted, also, that the international standard simplifies requirements.

What's more, organizations that have previously developed (or plan to develop) non-business continuity, ISO-compliant management systems (e.g. for asset management, service management, quality management, security management, environmental health and safety, etc.) will find it easier to integrate those systems with an ISO 22301-compliant BCMS.

But is ISO 22301 compliance overkill for smaller enterprises without an international footprint? Not at all. For starters, the risk of post-disaster business closures weighs heaviest on smaller businesses, making the need for a best-practice BCMS particularly acute. According to the U.S. Federal Emergency Management Agency, 40 to 60 percent of small businesses never reopen following a disaster.

40 to **60%** of small businesses never reopen following a disaster

As for ISO 22301, in particular, the standard is flexible by design. What does that mean, exactly? The specified requirements are generic. In other words, they are intended to be applicable to all organizations, irrespective of type, size, and nature. What governs actual application of the requirements, then, is the individual organization's operating environment. The opening passages of the standard, which detail its scope, make the point explicitly:

It is not the intent of this International Standard to imply uniformity in the structure of a Business Continuity Management System (BCMS), but for an organization to design a BCMS that is appropriate to its needs and that meets its interested parties' requirements. These needs are shaped by legal, regulatory, organizational and industry requirements, the products and services, the processes employed, the size and structure of the organization, and the requirements of its interested parties.

This International Standard is applicable to all types and sizes of organizations that wish to:

A. Establish, implement, maintain and improve a BCMS

B. Ensure conformity with stated business continuity policy

C. Demonstrate conformity to others

D. Seek certification/registration of its BCMS by an accredited third-party certification body

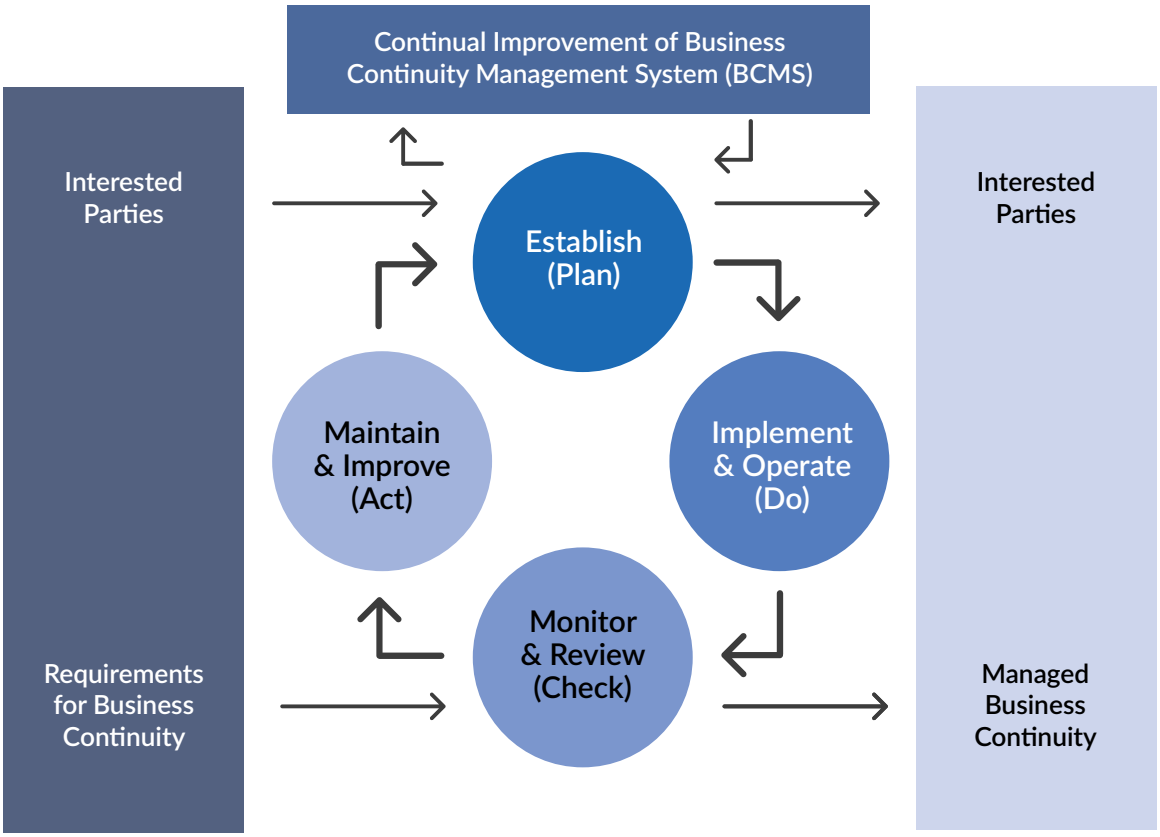
E. Make a self-determination and self-declaration of conformity with this International Standard

This International Standard can be used to assess an organization's ability to meet its own continuity needs and obligations[vi].

In essence, ISO 22301 applies to any and all organizations looking to establish, implement, maintain, or even just improve their BCMS. Therefore, it's a surefire way for those companies to ensure compliance with stated business continuity policies, whether those policies are internally mandated or dictated by external regulators, customers, or other parties. Independent of external mandates, too, compliance with ISO 22301 also helps organizations signal to prospective customers and partners their commitment to continuity of service. But remember, compliance with the standard can't just be a box-ticking exercise, especially if organizations seek to achieve organizational resilience and build the capability to respond effectively to major disruptive events.

The standard itself includes ten primary clauses, including the introduction, scope, normative references, and important terms and definitions sections. Like other international standards, ISO 22301 applies the "Plan-Do-Check-Act" (PDCA) model (depicted below). The model details the following:

Plan	Establish business continuity policy, objectives, targets, controls, processes, and procedures relevant to improving business continuity in order to deliver results that align with the organization's overall policies and objectives.
Do	Implement and operate the business continuity policy, controls, processes, and procedures.
Check	Monitor and review performance against business continuity policy and objectives, report the results to management for review, and determine and authorize actions for remediation and improvement.
Act	Maintain and improve the BCMS by taking corrective action, based on the results of management review and reappraising the scope of the BCMS and business continuity policy and objectives.



Source: International Standard Organisation

Unpacking the remaining clauses

The structure of the standard, consistent with that of other ISO management system standards, means that compliance entails full adherence with all specifications, not just a representative handful. To that end, the remaining sections of the standard, as well as main components therein, are as follows:

Context of the organization.
Effective business continuity management depends on a thorough understanding of an organization's internal and external needs. The task for business continuity professionals is to set clear boundaries for the scope of the eventual system, consonant with applicable legal and regulatory requirements.

Main components, here, include establishing and documenting the following:

- What the organization does, and the potential impact of disruptions
- Relationship with other policies and wider risk management
- Contractual and other requirements
- Who are the interested parties
- Scope of the management system

Leadership.
BCM is not a back-office activity. It requires serious, senior management engagement throughout the business continuity lifecycle. Specifically, senior management engagement is necessary for ensuring adequate BCM resourcing and staffing.

Main components, here, include establishing and documenting the following:

- Leadership and commitment with respect to Business Continuity Management
- A business continuity management policy
- Roles, responsibilities, and authorities

Planning.
An effective BCP begins with a thorough risk assessment and a rigorous business impact analysis (more below). Teams should also set out clear objectives and criteria to measure plan success.

Main components, here, include determining and documenting the following:

- Risks and opportunities presented by the objectives and requirements
- BC objectives and plans to achieve them
- Minimum acceptable levels of output
- Some form of project plan, with an evaluation mechanism

Support.
BCM doesn't happen in a vacuum. More than senior management engagement, organizations will need a stock of qualified professionals with relevant knowledge, skills, and experiences. Staff also needs to be apprised of their role in responding to incidents.

Main components, here, include establishing the following resources to support the BCMS:

- A competence system
- An awareness program
- A communications plan, to include both incident and non-incident situations
- Documentation and its management

Operation.
This clause lays out many of the requirements for the BCP, including the mandate to establish disruption and continuity management procedures.

Main components, here, include planning and implementing processes to deliver the following:

- Business impact analysis and risk assessment
- Strategies
- (Contingency) resources
- Impact mitigation
- Incident response structure and plans
- Exercise and test arrangements

Performance evaluation.
Developing a business continuity management system isn't enough. Organizations still have to monitor, measure, and evaluate their BCMS once it's in place. ISO 22301 stipulates calls out the necessity of internal audit programs.

Main components, here, include determining and documenting arrangements for the following:

- Monitoring, measurement, analysis, and evaluation
- Internal audit
- Management review

Improvement.
Organizations change, so too do the business environment around them. The BCMS needs to keep up with those changes. What's more, BCM teams must also identify nonconformities and take corrective actions to continue to enhance the overall performance of the BCMS.

Main components, here, include establishing procedures for the following:

- Non-conformance identification, reporting, and consequence control
- Corrective actions (system changes)
- Continual improvement

Understanding the Business Impact Analysis (BIA)

Usually undertaken by an internal governance committee, the business impact analysis (BIA) is a methodical accounting of business activities and the effect business disruptions would have on those activities. In the context of the BCMS and wider BCM program, the BIA is intended to help organizations isolate critical business functions in tandem with the processes and resources needed to support them.

Why is the BIA important? Well, firms might have a good feel for the services and products they need to continue delivering in order to avoid severe revenue loss in the event of a major disruption. But it's not a given that senior managers have a more nuanced understanding of the dependencies that underlie those services.

After all, a lot goes into moving a product: internal dependencies, like employee availability, corporate assets, and support services, as well as external dependencies, like suppliers. A good BIA will capture all of those contingencies, then rank the order of priority of services or products for continuous delivery or rapid recovery.

BIA findings then get fed into the BCP proper, which typically covers the resources, services, and activities required to ensure the continuity of critical business functions.

For businesses' implementing ISO 22301, it's vitally important that business process owners really engage with the risk analysis part of the BIA, rather than having it shunted to the side, undertaken in isolation in the Business Continuity Manager's Office.

In closing, rates of BCP adoption remain alarmingly low. But even for organizations who've successfully completed a BCP, or have procured business continuity solutions, the work to prepare your business for a major disruption isn't done yet. Many vendors have focused their BCP solutions exclusively on preventing data loss and the loss of IT systems. However, natural disasters and other catastrophic events can cause road closures, utility outages, the loss of key staff members, and critical supply problems, all leading to business failure. To be effective, BCM programs must be focused on broader issues than just data loss or temporary loss of access to IT systems.

As a BCM best-practice standard, ISO 22301 helps organizations identity what functions are essential. Risk management, then, helps businesses prioritize and develop mitigating controls. Finally, trainings of accessible procedures, pre-assigning roles and responsibilities, as well as exercises prepare people to know what to do during a disaster.

That's why having a BCP is one thing, executing that plan during a disaster quite another. Here, crisis and emergency management factor in heavily, i.e. during the response and recovery phases. Having an integrated safety and security system that turns your plans into actions based on pre-defined scenarios will facilitate speedy response and recovery.

Citations

i *Logan Sisam, Utah Division of Emergency Management: 75% of companies without business plans fail within three years after facing a disaster and or operational disruption. Available at https://www.utah.gov/beready/business/documents/newsletters/2015/november.pdf.*

ii *Jon Taiga: Disaster Recovery Planning: Managing Risk and Catastrophe in Information Systsems.*

iii *Jonathan Bernstein, Bernstein Crisis Management.*

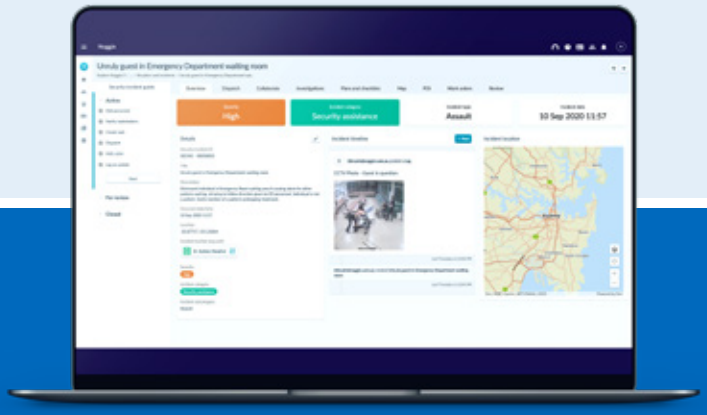
iv *HP and SCORE: Impact on U.S. Small Business of Natural & Man-Made Disasters. Available at https://waytek.com/wp-content/uploads/2015/03/HP_Download_ImpactofDisaster.pdf.*

v *Ibid.*

vi *Ibid.*

Like what you read?
Follow Noggin on social media

@teamnoggin facebook.com/teamnoggin linkedin.com/company/noggin-it



noggin
for Business Continuity

Meet the next-generation tool for corporate crisis and business continuity management teams to collaborate, plan, track their response, and share information. Built on the Noggin Core platform, Noggin Business Continuity gives response teams and decision makers the tools to know what's happening, collaborate quickly and effectively, make better decisions, and enact the right plans to take action when it counts the most.

The Noggin Business Continuity solution pack is backed by the Noggin Library with hundreds of plans and best-practice workflows, out of the box, and installed in minutes.

To learn more,
visit: **www.noggin.io**
or contact: **sales@noggin.io**