AVALUTION
CONSULTING

IMPLEMENTING ISO 22301

THE BUSINESS CONTINUITY MANAGEMENT SYSTEM STANDARD

BRIAN ZAWADA & GREG MARBAIS, AVALUTION CONSULTING

The business continuity community has been anticipating the release of ISO 22301 (Societal security – Business continuity management system – Requirements) for years as a unifying standard that crosses international borders. Using simple, straightforward language, ISO 22301 summarizes minimum requirements for effective business continuity and can enable coordinated preparedness among diverse organizations around the world. Overall, ISO 22301 offers a unique value proposition that will drive higher levels of business continuity performance in years to come.

BEFORE YOU BEGIN READING

Organizations with a strong understanding of management systems realize the most value from ISO 22301, but we recognize that not everyone is familiar with management systems and their related processes. As such, this white paper is organized into three sections:

SECTION 1: INTRODUCTION TO ISO 22301
This section provides an overview of the standard, including its scope, audience, and value proposition.

SECTION 2: WHAT IS A MANAGEMENT SYSTEM?
This section introduces key management system concepts that all business continuity professionals should understand before moving forward with the implementation of ISO 22301.

SECTION 3: UNDERSTANDING ISO 22301'S STRUCTURE AND CONTENT
This section focuses solely on ISO 22301, introducing practical, pragmatic guidance to successfully implement the standard and take advantage of each element of the business continuity management system.

Throughout this white paper, we've included a number of links to related content published by our consultants. Consider clicking on these links for more in-depth information on these subjects.

CONTENTS

For additional business continuity and IT disaster recovery-related resources, check out Avalution's blog: **perspectives.avalution.com**

SECTION 1
INTRODUCTION TO ISO 22301

SCOPE OF THE STANDARD

As stated in ISO 22301 Clause 1, the intended purpose of the standard is to enable organizations to "protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise" by establishing, operating, and continuously improving a business continuity management system (BCMS).

The official title of ISO 22301 reflects that it is a "requirements" document, but what exactly does that mean? Essentially, standards are structured in one of two ways:

- **REQUIREMENTS STANDARDS:** A document written in a way that captures core elements of a discipline that should be implemented regardless of an organization's size, location or purpose (industry). In other words, requirements standards detail "what" an organization should do, not necessarily "how" they should do it. Written using the word "shall," requirements standards enable independent audit and certification (if a business case warrants such a decision).

- **GUIDANCE STANDARDS:** Designed to complement a requirements standard or act in a purely independent manner, guidance standards detail more of the "how" by introducing implementation strategy options based on best practices. In the case of business continuity, ISO 22313 is the guidance standard that supports ISO 22301 by offering implementation and continual improvement strategies.

Again, ISO 22301 is a requirements standard, written to enable auditability, as well as organizational certification for entities seeking such third-party, independent attestation. Certification, while optional, is a value-adding differentiator for many organizations, particularly those engaged in business-to-business transactions, as it provides third-party validation of the effectiveness of the organization's business continuity management system. However, first and foremost, ISO 22301 was written to enable higher levels of business continuity performance, and Avalution expects that the vast majority of organizations will align to the spirit and intent of the standard for that reason.

The business continuity community has some fairly high expectations for ISO 22301. Avalution believes that the actual reaction will be mixed because some expectations often fail to align with the intent behind ISO-authored standards, in particular "requirements" standards. Already, many business continuity professionals feel the content in ISO 22301 is too high-level; many are looking for standards that address all possible needs for all organizations. ISO standards follow a rigorous, consensus-driven process that leads to content applicable to all organizations – regardless of geography, size, structure, or purpose, including not-for-profit entities and those in the public and private sectors. As such, ISO 22301 is written in a manner that introduces topics so the wording is applicable to everyone. In other words, the content is high-level and describes the ***what***, not the ***how***.

AUDIENCE

ISO 22301 describes business continuity planning concepts using clear, straightforward language that can be used by anyone in any organization to plan for, implement, and continually improve a business continuity management system. Regardless of experience or job title, ISO 22301 enables those charged with leading the business continuity planning effort to understand business continuity concepts with significantly less jargon and using descriptions in lieu of acronyms.

Ultimately, any entity and personnel (including business continuity professionals, program sponsors and executive management) charged with preparing for disruptive incidents will benefit from ISO 22301 if they intend to:

- Improve performance as it pertains to preparedness for a disruptive incident;
- Use approaches consistent with those employed by business partners and customers;
- Prepare for certification to the standard, if a business case exists (optional).

To be clear, this standard is not just for those brand new to the business continuity profession, nor is it strictly for the most experienced professionals. This standard is written for everyone with a role in mitigating risk associated with disruptive incidents.

ISO 22301'S VALUE PROPOSITION

Standards exist to improve organizational performance in a specific discipline. As an extension of performance improvement, standards are designed to offer approaches and solutions to address the most common challenges facing an organization. ISO 22301 is no different.

As the first international standard focused exclusively on business continuity planning, ISO 22301 offers content to address the most common challenges facing the organization as a whole, as well as its business continuity professional(s) and executive sponsors. In addition, the standard provides a framework to build the capability necessary to respond to, recover from, and operate effectively during the most challenging and unexpected circumstances.

Avalution identified seven key challenges that ISO 22301 is well-positioned to address:

1. **CLARITY REGARDING BUSINESS CONTINUITY OUTCOMES:** To executive management, the business continuity outcome is not recovery time and recovery point objectives, or even up-to-date plans. These are all necessary, but they are means to an end. Mitigating the risk of a disruptive incident and ensuring processes and resources are recoverable in order to meet interested party expectations specific to product/service delivery is not only the outcome executive sponsors expect, but what they want measured.

2. **FOCUS AND STRATEGIC ALIGNMENT:** The standard focuses on an organization's most important products and services, which forces scoping using the same methods the organization uses to measure and improve organizational performance in general. This approach helps executives connect risk and impact to organizational initiatives, objectives, and obligations.

3. **MANAGEMENT ENGAGEMENT:** Using management system concepts mapped to the Plan-Do-Check-Act (PDCA) model, this standard appropriately engages management and positions senior leadership to participate in the process of strategically scoping and setting objectives, making strategic resourcing decisions, and prioritizing continual improvement opportunities based on performance compared to objectives and needs.

4. **PERCEIVED COMPLEXITY:** Unfortunately, business continuity can often be perceived by many as overly complex and burdensome. ISO 22301 was written to focus on the most important methods to connect (and stay connected) with management and perform the activities that lead to higher levels of business continuity performance. In most cases, the standard avoids the use of unnecessary actions and acronyms. This approach contributes to diminished participant intimidation.

If done correctly, organizations will assess risk in terms of an inability to recover the activities and resources that deliver the organization's most important products and services, which is a powerful presentation for an executive management audience.

5. **INTEGRATION:** A growing number of organizations are integrating business continuity with other risk management disciplines, which demonstrates that the industry is maturing and becoming more accepted by executive management. As a management systems standard, ISO 22301 can help organizations appropriately coordinate risk management efforts, with the end objective of mitigating a broad range of risks in the most efficient manner possible.

6. **ADDRESSING MULTIPLE SOURCES OF NEEDS AND OBLIGATIONS:** Management systems standards are designed to be "plug and play." Because ISO standards are written on the international stage using consensus-driven approaches, they cannot possibly meet the unique needs of all organizations (be that legal, contractual, regulatory, or cultural). Instead, ISO management systems standards enable organizations to identify and address these influencing factors and obligations without directly calling out what they may be or what their requirements are.

7. **PROJECT VERSUS PROGRAM MINDSET:** ISO 22301 is all about continual improvement. With this as the focus, the risk of treating business continuity as a one-time action greatly decreases. It is clear to planning participants and their executive sponsors that recurring action is necessary to enable alignment to key priorities and the expectations of interested parties.

Since this standard involved input from over 60 countries, as well as multiple observer organizations over a number of years, it is safe to say that ISO 22301 summarizes best practices applicable to all entities, regardless of location, purpose, or size. For those struggling with selling certain business continuity planning approaches or techniques, ISO 22301 can serve as a form of benchmarking, summarizing the core planning activities necessary to ensure successful preparedness outcomes. Overall, ISO 22301 describes planning approaches and outcomes that lead to better uniformity and coordination with other interested parties, including government, customers, and suppliers. This new standard also focuses on response and recovery solutions performance (e.g., how fast and to what capability an organization can recover its most important activities and resources), not just how good the organization is at performing the business continuity planning lifecycle. If done correctly, organizations will assess risk in terms of an inability to recover the

activities and resources that deliver the organization's most important products and services, which is a powerful presentation for an executive management audience.

As a strong proponent of standards in general, and especially management systems standards, Avalution believes that ISO 22301 offers unprecedented value because of:

- ISO clout and acceptance
- Management engagement
- Clarity regarding business continuity scope (products and services)
- Continual improvement
- Performance-based content

Overall, this standard was developed to address some of the most significant, recurring obstacles that often lead to business continuity performance issues, specifically clarity of purpose and management engagement.

ISO 22301 AT A GLANCE

WHAT IS IT?

The first international standard focused exclusively on business continuity

WHAT IS THE SCOPE?

Implementing, operating, and continuously improving a business continuity management system

WHAT IS THE FOCUS?

Written for any organization, regardless of industry, size, or location

WHAT IS THE PURPOSE?

A requirements document; although written to drive business continuity performance, it supports voluntary organization certification

WHERE CAN I PURCHASE A COPY OF THE STANDARD?

ISO 22301: 2012 can be purchased here.

SECTION 2
WHAT IS A MANAGEMENT SYSTEM?

Although widely used in other professional disciplines for many years (i.e., quality, environmental, health and safety, and information security management), the term "management system" remains a relatively new concept to business continuity professionals. First introduced to business continuity professionals through British Standard (BS) 25999-2 as a business continuity management system, the management systems concept continues to gain traction in our profession through the ISO standards development effort, as well as new and updated standards from the National Fire Protection Association (NFPA) and ASIS International.

A management system is defined as the framework of processes and procedures used to ensure that an organization can fulfill all tasks required to achieve a set of related business objectives. Management system standards provide a model for establishing, operating, maintaining, and improving a management system and executing capabilities that align to management's expectations.

WHY SHOULD CONTINUITY PROFESSIONALS CARE ABOUT MANAGEMENT SYSTEMS?

Understanding management system principles is a key success factor in achieving the most value from ISO 22301. Even more importantly, many executive leadership teams may already be familiar with management system concepts and understand their role in operating within a management system. As discussed throughout this white paper, a management system is not only a great way to capture leadership support, but it's also a great way to keep it.

KEY CHARACTERISTICS OF MANAGEMENT SYSTEMS

A management system exists to continuously improve key processes and outcomes in order to meet core business objectives. But, what are some of the key characteristics of a management system, regardless of its focus?

1. **ACCOUNTABILITY:** A management system always outlines roles and responsibilities for its key interested parties, ranging from the most senior managers (often called "top management" in ISO standards) to the general employee population, as well as external entities that have a role in planning, response, and recovery.

2. **REPEATABLE PROCESSES:** Processes are not designed for one-time use; rather, they are designed to be revisited on a periodic basis in order to adapt the management system's outputs to organizational change.

3. **DOCUMENTATION:** Management systems enable repeatability through management-approved documentation that outlines expectations and process characteristics. Organizations also develop documentation in the form of standard operating procedures, or SOPs (in some organizations, SOPs are called frameworks), which set specific performance and frequency expectations to ensure repeatability and continual improvement.

4. **RESOURCES:** A management system identifies the resources needed to enable alignment with organizational objectives.

5. **PERFORMANCE MEASUREMENT AND REVIEW MECHANISMS:** With a focus on continual improvement, a management system includes methods of assessing performance based on senior leadership's expectations.

6. **COMPETENCE:** A management system defines the role-specific skills and experiences necessary to meet objectives.

7. **CULTURAL CHANGE:** Building, promoting, and embedding a business continuity management culture within an organization through training and appropriate communications mechanisms ensures that it becomes part of the organization's core values and, perhaps, even part of its governance structure. In other words, business continuity stops being a series of separate activities and becomes part of day-to-day decision-making and operations instead.

KEY COMPONENTS OF MANAGEMENT SYSTEMS

All management systems standards include ten key components. In the case of ISO 22301, each component is designed to provide value to the organization as described in the following list:

1. **POLICY AND OTHER DOCUMENTATION:** Documentation includes written, management-endorsed expectations and procedures designed to drive repeatable performance and continual improvement.

2. **LEADERSHIP INVOLVEMENT:** In order to drive alignment with strategic needs and imperatives, executive management must be involved with scoping and objectives-setting from the beginning. This involvement enables management to continuously allocate resources and prioritize continual improvement opportunities based on scope change and performance measurement results.

3. **CONTEXT AND OBLIGATIONS:** As mentioned earlier, management systems essentially demand that organizations establish a scope based on key products and services rather than facilities or the organizational chart. This approach is not only more strategic, but also enables effective dialogue with executive managers because they think in terms of organizational outputs (products and services). Management systems also involve identifying obligations (legal, regulatory, and contractual) up front as a source of requirements. "Context definition" is a continuous process, reviewing in-scope products, services, and associated obligations, which is key to establishing a constant connection between the organization's strategic needs and the business continuity management system.

4. **RESOURCES:** This category includes both the time and money necessary to enable personnel charged with business continuity planning to meet objectives based on the scope established by executive management.

5. **COMMUNICATION:** Business continuity planning activities and solutions require coordination and introduction to all interested parties. Communication can take the form of instructing employees regarding planning activities or developing awareness regarding response and recovery strategies, as well as internal and external communication when faced with a disruptive incident.

6. **COMPETENCIES / TRAINING AND AWARENESS:** In order to perform based on expectations, personnel assigned to specific business continuity planning activities must have the right skills and experiences to be successful. As such, management systems involve defining roles and competencies (qualifications), as well as the training and awareness content necessary to build and grow competencies.

7. **PERFORMANCE EVALUATION AND INTERNAL AUDIT:** This element involves evaluating performance based on management's expectations (which may include the use of Internal Audit or independent, objective parties) and creating processes to communicate feedback.

Organizations struggling to capture and keep senior leadership's attention will quickly realize value when implementing management system concepts – positive input and feedback will increase, as will the resources necessary to meet management expectations.

8. **NONCONFORMITY AND CORRECTIVE ACTIONS:** This management systems element identifies where business continuity planning activities and solutions fail to meet policy and other obligations, as well as sets performance targets (in this case, recovery objectives or risk mitigation targets).

9. **MANAGEMENT REVIEW:** This activity enables formal methods of communicating management system characteristics and performance in order to capture management feedback and approval.

10. **CONTINUOUS IMPROVEMENT:** This activity enables the program to internalize performance feedback in order to improve key processes and outcomes, thus more closely aligning to the strategic needs of the organization.

THE RELATIONSHIP OF MANAGEMENT SYSTEMS TO PDCA

Those familiar with management systems often equate them to something known as a "Plan, Do, Check, Act" systems methodology, or PDCA. This iterative, flexible methodology and its general concepts originated with Total Quality Management (TQM). It was made popular by Dr. W. Edwards Deming, who is considered by many to be the father of modern quality assurance. PDCA weaves decision making into the fabric of an organization's overall operational capability and business practices, and often makes the organization more efficient and better positioned to meet important challenges. PDCA provides a problem identification and problem solving method that can be implemented by an organization in many different ways, depending on its unique activities and needs. Executing the cycle over time extends knowledge about the PDCA process. As such, repeating the PDCA cycle continuously can bring an organization closer to its goals, usually ideal operational capability and high quality outputs.

By incorporating PDCA into business continuity management, organizations can assess their unique needs to make informed decisions. As has been demonstrated with environmental and quality management standards, the PDCA approach creates an organizational culture that drives continual improvement through repetitive performance measurement and feedback.

The following graphic maps ISO 22301's ten clauses to the PDCA model:

INTRODUCTION

- Clause 1: Scope
- Clause 2: Normative References
- Clause 3: Terms and Definitions

REQUIREMENTS

- Clause 4: Context of the Organization ..... **PLAN**
- Clause 5: Leadership ..... **PLAN**
- Clause 6: Planning ..... **PLAN**
- Clause 7: Support ..... **PLAN**
- Clause 8: Operations ..... **DO**
- Clause 9: Performance Evaluation ..... **CHECK**
- Clause 10: Improvement ..... **ACT**

Most of what business continuity professionals consider as traditional business continuity methodology resides in "Do," whereas the set-up and continual improvement of the management system resides in "Plan," "Check," and "Act."

HOW DO MANAGEMENT SYSTEMS APPLY TO BUSINESS CONTINUITY?

Risk management efforts are greatly enhanced with management-oriented models that avoid professional jargon and focus on organizational outcomes. As described above, PDCA is simple to understand, proven, and widely accepted as a means of engaging management. Further, it lends itself to multi-disciplinary application and coordination. Management systems offer a series of processes wrapped around a common objective, and, in the case of business continuity management, the objective is mitigating business continuity-related risk, which includes protecting the activities and resources that deliver the organization's most important products and services.

Management systems add value because, by design, they enable an organization to address multiple standards, regulatory requirements, and other obligations. In the case of business continuity, organizations often have multiple sources of requirements influencing the execution of planning activities. Because management systems standards such as ISO 22301 can help implement an "umbrella" management system, it is well-positioned to flexibly serve every organization's unique business continuity needs, as they are free to add planning activities and solutions to the business continuity management system.

WHAT'S THE RELATIONSHIP BETWEEN A BUSINESS CONTINUITY PROGRAM AND A BUSINESS CONTINUITY MANAGEMENT SYSTEM?

Many managers and business continuity professionals see little difference between a business continuity program and management system, but, in reality, the subtle differences can lead to major performance improvements.

A program is a planned sequence and combination of activities designed to achieve specific goals. A program normally involves organizing resources to perform a finite, recurring set of activities to meet a set of specific objectives (sometimes performed alone and without coordination with other processes, activities, or disciplines). However, this approach often does little to evaluate, incorporate, and address the wider organizational obligations, activities, and needs.

In comparison, a management system refers to what the organization does to define and manage its processes and activities so its products and services meet the objectives it has set for itself, such as:

- Satisfying the customer's requirements;
- Capturing market share or offering a competitive differentiator;
- Complying with regulations; or
- Meeting other organizational objectives.

Management systems offer a proven, discipline-neutral framework for managing and continually improving an organization's policies, processes, and activities, as well as the outcomes specific to the discipline.

It is a common misconception that an organization must use one or the other – either a program or a management system. Interestingly, what many business continuity professionals view as program approaches for preparedness (risk assessments, business impact analyses, plan documentation, exercises, and maintenance processes), ISO 22301 still includes (essentially Clause 8 of the standard); however, these aspects are just part of the overall approach, making up the "Do" of PDCA. The remaining management system concepts drive management connection, strategic alignment, continuous improvement, and repeatability.

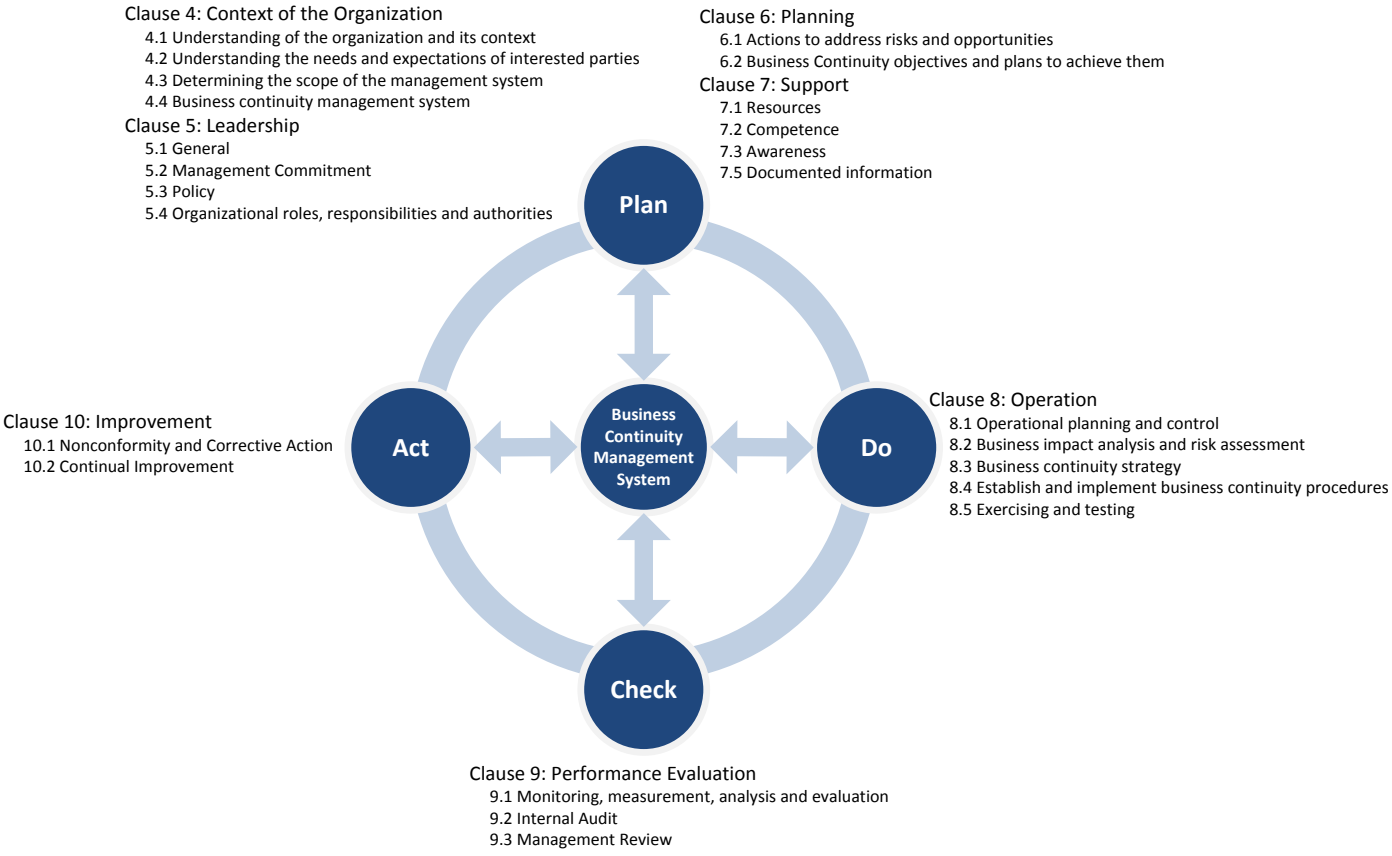
WHERE CAN I GO FOR MORE INFORMATION ON MANAGEMENT SYSTEMS?

A number of resources are available to further describe management systems. Consider purchasing a copy of ISO Guide 72, which offers considerable information on key management system components and characteristics. Also, review other management systems-oriented standards (BS 25999-2, ISO 9001, ISO 14001, ISO 27001), or consult with Quality, EHS, or Information Security professionals that have experience developing, implementing, or operating management systems. Lastly, review the numerous management system case studies posted online in order to further understand the value of the concept and how organizations have achieved success.

Overall, management systems are now part of the business continuity profession, and Avalution believes the industry is fortunate that these concepts are now becoming the status quo within industry standards. Organizations struggling to capture and keep senior leadership's attention will quickly realize value when implementing management system concepts – positive input and feedback will increase, as will the resources necessary to meet management expectations.

SECTION 3
UNDERSTANDING ISO 22301'S STRUCTURE & CONTENT

The ISO 22301 standard is the first international standard organized using the new Joint Technical Coordinating Group (JTCG) structure as documented in ISO Guide 83, which will serve as the structure for all new or revised management systems standards. This new structure includes ten clauses (or sections). The first three clauses of the standard provide background information regarding ISO 22301. Clauses four through ten define the business continuity management system. The following graphic shows how the clauses align to the Plan-Do-Check-Act model:



This section of the white paper offers a detailed description of the ten clauses in ISO 22301. Starting with Clause 4, Avalution structured the summary of each clause by focusing on four topics:

WHAT IS IT?

TIPS ON GETTING STARTED

WHAT VALUE CAN IT DELIVER?

BEFORE MOVING ON

ISO 22301 – THE INTRODUCTION AND THE FIRST THREE CLAUSES

Before capturing the actual requirements of the standard, ISO 22301 first starts with an introduction, a description of the scope of the standard, a section highlighting normative references, and a list of terms and definitions. It is important to understand, at a high level, the content in the introduction and each of the first three clauses. The table below offers a brief description of each clause, as well as a brief summary of the content Avalution feels is most important.

CLAUSE	WHAT IS IT?	WHAT YOU NEED TO KNOW
Introduction	Setting the tone for ISO 22301, the introductory clause offers perspective on the importance of a business continuity management system, its key components, and how this standard aligns with the Plan-Do-Check Act model.	This is a management systems standard, which focuses on ensuring a proper alignment between the organization and business continuity activities, solutions, and expectations, as well as driving continual improvement.
I. Scope	Clause 1 describes the scope of the standard. The key words found in this section include, "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."	The scope of this standard is implementing and improving a business continuity management system. The standard's authors sought to ensure that the content applies to all organizations, regardless of geography, size, or purpose.
II. Normative References	In ISO language, normative references refer to other documents or content that the reader must understand or have access to in order to understand this document.	As ISO 22301 does not have any normative references, this clause is essentially a blank part of the ISO standards template. Although ISO 22313 helps ISO 22301 users understand how to implement a business continuity management system, it is not a mandatory document necessary to successfully use this standard.
III. Terms and Definitions	This section offers definitions for each of the terms used in ISO 22301, as well as the terms used in the ISO 22313 guidance document.	ISO 22301 includes 55 terms and definitions, many of which are found in other societal security or risk management standards, including ISO 31000.

ISO 22301 – CLAUSE 4 – CONTEXT OF THE ORGANIZATION

PLAN DO CHECK ACT

WHAT IS IT?

Clause 4 involves defining and understanding the context of the organization. This awareness step helps management and those charged with performing business continuity planning define the obligations that should influence the identification of BCMS objectives.

An effective BCMS will consider the following when establishing objectives:

- Legal, regulatory, and contractual requirements;
- All internal and external parties that have an interest in the organization's business continuity efforts; and
- The organization's strategic objectives, policies, priorities, and risk appetite.

In addition to understanding requirements, it is important that the organization also identify and understand the expectations of any parties that have an interest in the BCMS (known as interested parties, previously described in management system standards as stakeholders), as well as understand how processes and activities, supply chains, and partnerships all contribute to influencing and meeting objectives.

Organizations should only establish the scope of their BCMS after assessing the context of the organization. Why? To ensure that the scope properly considers the organization's requirements and identifies its most important products and services.

WHAT VALUE CAN IT DELIVER?

Clause 4 works to understand organizational and environmental obligations and objectives (thus understanding how the BCMS should apply to the context of the organization). By evaluating organizational need, the environment, and interested party expectations, the business continuity management system will have the foundational information necessary to establish an appropriate scope and set of objectives.

TIPS ON GETTING STARTED

To align with the requirements outlined in Clause 4 of ISO 22301, Avalution recommends following this four-step process:

1. **Review Documentation:** Collect information specific to the current mission and strategy of the organization. Most organizations publish (at least internally) documents that discuss the mission, strategy, and goals of the organization. Many organizations also have public information available, such as annual reports and website content describing products and services. These documents and sources of information will help to identify organizational priorities and requirements. This preliminary document review will contribute to framing the scope of the BCMS.

2. **Discuss With Management:** As the documents and information collected in step 1 may be outdated (or at least infrequently updated), work with the organization's senior leadership team to identify changes to the organization's mission and strategy, as well as long-term growth goals and forecasts. Interviewing executives can be completed one-on-one if necessary, but the best results come from facilitating a group discussion. While not always feasible because of the busy schedules of senior executives, a group discussion on the organization's priorities and risk appetite will result in the most thorough understanding of the organization's context for the BCMS.

3. **Identify Products and Services:** Define the scope of the BCMS in terms of products and services. Once an organization understands its context, it should be possible to identify the products and services to include in the scope of the BCMS. The scope should also be adapted to the size and nature of the organization, as well as the maturity of the organization's BCMS. Organizations that are new to business continuity may start with just the highest priority products and services as in-scope and add other products and services as the BCMS matures over time. Smaller organizations may be able to define the scope of the BCMS to cover all products and services. Regardless of the number of products and services defined as in-scope, the most important point to remember is that an appropriately defined scope will permit a manageable implementation of the BCMS positioned for continual improvement (and expansion, if necessary) over time.

4. **Define Risk Appetite:** Many professionals currently evaluating ISO 22301 have questions regarding the concept of risk appetite, which is introduced in Clause 4. Unfortunately, the concept is not defined in ISO 22301. As such, take some time to understand this concept as it is described in ISO 31000 and work to define your organization's risk appetite as it pertains to business continuity. Avalution recently published an article on this topic, titled: How to Determine Risk Appetite in the Context of Business Continuity.

BEFORE MOVING ON TO "LEADERSHIP"

Although the "context" phase may seem relatively easy and straightforward, it is critical to apply an appropriate level of focus and effort because the scope of the BCMS will influence all efforts in subsequent phases. Further, defining the scope through products and services enables a focused approach to engage the most appropriate business leaders for subsequent assessment and strategy development activities.

ISO 22301 – CLAUSE 5 – LEADERSHIP

PLAN DO CHECK ACT

WHAT IS IT?

Clause 5 establishes the requirements for leadership of the BCMS – defining the key activities that top management must perform to guide the alignment of business continuity efforts with broader organizational strategy, as well as ensuring the management system has the necessary support to be successful. Beyond providing visible support and serving as a champion for implementation and continual improvement, ISO 22301 states that top management (leadership) is responsible for establishing a business continuity policy, assigning roles and responsibilities, and promoting continual improvement. The following information provides a brief explanation of these two requirements:

- **Business Continuity Policy:** A business continuity policy statement demonstrates commitment to the BCMS, documenting performance objectives and enabling the active communication of expectations throughout the organization.

- **Organizational Roles, Responsibilities, and Authorities:** Leadership will assign roles as necessary to implement and continually improve the BCMS, including providing the necessary authority to perform those roles. In addition, leadership will assign responsibility for reporting to top management on the performance of the BCMS.

WHAT VALUE CAN IT DELIVER?

Clause 5 is not the only section in the standard that describes leadership responsibilities, as top management roles and responsibilities are found throughout the document. However, dedicating a section to leadership demonstrates the importance that leadership has in the success of a BCMS. Clause 5 also clearly states that a well-defined and carefully-crafted policy statement can serve as an effective vehicle to promote business continuity and set expectations, including who should perform an active role in the planning effort.

TIPS ON GETTING STARTED

To align with the requirements outlined in Clause 5 of ISO 22301, Avalution recommends following this three-step process:

1. **Establish a Business Continuity Steering Committee (BCSC):** A one-size-fits-all approach to implement a BCMS leadership structure does not exist. However, regardless of the name or structure of the leadership team, an appropriately chartered BCSC serves as a representative source of information from each area of the organization to guide business continuity efforts, while also advocating for business continuity in their respective areas. The BCSC is a group representing or comprised of senior management that is responsible for overseeing the BCMS, supporting the business continuity efforts of the organization, and allocating the necessary resources to meet business continuity objectives. The scope of the BCMS helps identify all of the business units or divisions that should be represented on the BCSC. A comprehensive yet focused business continuity steering committee helps ensure the interests of the business are represented in BCMS decision-

making, obtain feedback from the organization, and communicate the importance of contributing to the BCMS.

2. **Create a Business Continuity Policy:** The business continuity policy establishes and conveys the basic framework for business continuity planning in a concise manner. The policy should communicate scope (products and services, as well as which areas of the organization are to be included), business continuity performance objectives, measures to gauge performance, intervals for reporting to management about performance, a commitment to continually improving the BCMS, and define roles and responsibilities (ranging from top management through the general employee population).

3. **Establish Roles and Responsibilities Necessary to Execute the BCMS:** The roles used in a BCMS will vary by organization, with certain individuals potentially performing multiple roles. Each organization should structure the roles and responsibilities in a way that fits the organization, yet still accomplishes the objectives of the BCMS. Two common roles are the sponsor and coordinator.

    - **Sponsor:** The sponsor is a senior level executive with overall accountability for business continuity performance and nearly always has other responsibilities in the organization. This person should have the authority to make decisions necessary to implement and continually improve the BCMS, as well as the influence in the organization to assist in embedding business continuity in the organization's culture.

    - **Coordinator:** The coordinator is responsible for overseeing and influencing the day-to-day operation of the business continuity planning effort. The coordinator is responsible for executing the BCMS as directed by the BCSC while the sponsor (in most cases) serves as an advisor and overall decision-maker for business continuity planning activities taking place throughout the organization.

BEFORE MOVING ON TO "PLANNING"

The BCSC plays an integral role in rolling out and maintaining an effective BCMS. The BCSC becomes a conduit of information from those executing business continuity planning activities to the rest of the organization while returning the necessary feedback (business requirements and opportunities for improvement). Selecting the appropriate senior leadership to represent the organization on the BCSC is essential to gaining buy-in from personnel throughout the organization. With the right BCSC, policy, roles, and overall performance of the business continuity planning effort will appropriately reflect the needs of the organization.

ISO 22301 – CLAUSE 6 – PLANNING

PLAN DO CHECK ACT

WHAT IS IT?

At first glance, many business continuity professionals may associate the "planning" section of ISO 22301 with the generation of response and recovery plans; however, in ISO 22301, this concept is actually addressed in Clause 8. In this standard, Clause 6 is designed to plan the implementation of the BCMS based on organization-wide requirements and the scope defined in Clause 4 (Context). The planning explained in this clause results in the creation of a BCMS structure and approach that aligns to the organization's strategy and culture. The requirements found in this clause also define BCMS objectives (as opposed to recovery time and recovery point objectives), which enable expectations to be met and allow performance measurement.

WHAT VALUE CAN IT DELIVER?

Two common objections to or issues with business continuity planning include:

1. A perception that organizational risk management disciplines are too different to coordinate; or
2. Business personnel will demand overly aggressive recovery objectives without guidance.

Perhaps a more appropriate title for Clause 6 would be "approach," as this clause seeks to help organizations flexibly implement business continuity and ensure that the more tactical planning efforts (such as the business impact analysis) have the appropriate guidance to be successful and align to management expectations.

TIPS ON GETTING STARTED

To align with the requirements noted in Clause 6 of ISO 22301, Avalution recommends following this three-step process:

1. **Define BCMS Objectives:** Using the organization's BCMS scope statement developed in Clause 4, work with your business continuity steering committee to define BCMS objectives, and then socialize these objectives among those responsible for executing the business continuity lifecycle.

   As an example, Avalution has listed some of its BCMS objectives below to demonstrate internal priorities (keep in mind that this is a sub-set of our BCMS objectives, others include maximum downtime tolerance for each of our client-facing products and services):

   - Protecting the safety of Avalution's employees and visitors.
   - Managing the threats and impacts associated with an interruption to critical operations, including a facility interruption or loss of resources (including personnel, technologies and business partners).
   - Reducing business continuity risk through four approaches:

- An appropriate and proactive control environment designed to decrease the likelihood of a disruptive event;
- Strategies to effectively respond to a crisis;
- Plans to recover critical business activities within stakeholder expectations; and
- The ability to maintain consistent communication with personnel and clients.

When defining BCMS objectives, ensure they align to the scope of the BCMS, the boundaries of the planning effort, and the expectations and requirements of all interested parties.

2. **Align with Other Risk Management Disciplines:** Identify related risk management disciplines that, if coordinated with, would enable a more efficient preparedness effort. If others perform risk assessments in line with ISO 22301 and ISO 31000, for example, don't reinvent the wheel – leverage the results! Do not mitigate risks multiple times – pick the best, most effective approach. Lastly, consider a single management system for the treatment of risk (with each risk area owning the execution, presentation, and incorporation of management feedback into their respective areas), and leverage senior leaders willing to contribute to the control of risk.

3. **Align with Organizational Culture:** Define how to perform business continuity planning based on available resources (centralized and decentralized), organizational culture, and organizational structure. Identify the best way to involve business continuity planning in day-to-day operations, project management, and change management.

BEFORE MOVING ON TO "SUPPORT"

Creating objectives for the organization as a whole and preparing to communicate the results to those involved in planning is a key success factor. Objectives should be stated in a way that make it possible to measure success, failure, and progress towards completion. One other key characteristic is clarity. Ambiguous objectives that are difficult to measure will often result in push back from the personnel assigned to achieve the objectives. Although clear goals do not guarantee buy-in from all personnel involved in the BCMS, ambiguous objectives will increase opposition to the BCMS.

ISO 22301 – CLAUSE 7 – SUPPORT

PLAN DO CHECK ACT

WHAT IS IT?

Support is the final ISO 22301 clause that completes the "Plan" phase of the PDCA model in the standard. Clauses 4 through 6 establish what the BCMS is to accomplish, while Clause 7 assigns resources to allow an organization to implement, maintain, and continually improve the BCMS, including:

- **Personnel Competency:** Determine the necessary knowledge and experiences (by role) needed to plan for, respond to, and recover from disruptive incidents. For roles where personnel do not currently possess the necessary competencies, provide training opportunities to fill any gaps.

- **Awareness:** Promote awareness of the business continuity policy to all personnel, as well as how each person contributes to the success of the BCMS. Additionally, make sure that all personnel with a role in the business continuity management system understand the implications of not meeting expectations, as well as their role following the onset of disruptive incidents.

- **Communication:** Create a communications plan for the BCMS, which includes communications during the planning effort (pre-incident) as well as following the onset of a disruptive incident. The communications plan will consider both internal and external interested parties and identify appropriate messaging and methods of communications. This section of the standard raises some new and interesting requirements when compared to other standards, and calls out the need to integrate with national and regional warning systems, as well as the need to maintain procedures to test communications mechanisms.

  For more information on this topic, read: Crisis Communications: An Organizational Balancing Act

- **Documentation:** Ensure proper documentation of BCMS activities, documents, approval, and communication. Following the release of ISO 22301, a number of experts commented that this new standard required far more documentation. It is Avalution's position that nothing has changed. Avalution assumed processes described in other standards like BS-25999-2 and NFPA 1600 required documentation to ensure repeatability; ISO 22301 formally states the requirement for BCMS process documentation, as well as documentation describing outcomes. Additionally, Clause 7 describes requirements for document management, access, retention, and protection.

WHAT VALUE CAN IT DELIVER?

Clause 7 seeks to address the all-too-common issue of management mandates with inadequate resources by formally defining the process and expectations around review and commitment of the resources (people, budget, and time) necessary to ensure success. As this is a management system, communications and documentation are keys to success as well. Addressing the requirements in Clause 7 will help proactively address the risk of a poorly resourced, communicated, and documented risk management discipline.

TIPS ON GETTING STARTED

To align with the requirements outlines in Clause 7 of ISO 22301, Avalution recommends following this five-step process:

1. **Document Standard Operating Procedures:** Beyond writing plans to respond and recover following a disruptive incident (addressed in Clause 8), carefully document how you intend to comply with ISO 22301. As noted earlier in this white paper, this is often called a Standard Operating Procedure, or SOP. Some organizations may call this documentation a framework or standard. Regardless, document the recurring nature of the activities that comprise the BCMS, being more detailed than the content summarized in the policy statement.

2. **Create a Competency Assessment and Development Program:** All personnel with a role in the BCMS, including those with a role in the response and recovery planning process (addressed in Clause 8), require certain competencies necessary to fulfill their role's responsibilities. The assessment and development program should regularly identify necessary competencies as well as the corresponding development opportunities when gaps are identified. The program should maintain the appropriate records relating to competencies and development activities. For each role, Avalution recommends documenting the following:

    - Responsibilities
    - Competencies
        i. Education
        ii. Knowledge
        iii. Experience
        iv. Skills
        v. Training

3. **Develop a Communications Plan:** A communications plan informs interested parties about the BCMS. The communications plan should summarize key messages that the organization intends to convey regarding the planning process and its capabilities, as well as how these messages should be conveyed, when, and to whom. Interested parties include internal audiences (such as all employees, senior managers, boards of directors, and response/recovery teams), as well as external audiences (such as customers, suppliers, and partners), and local community organizations (such as government decision-makers and first responders). Some key messages for internal and external audiences are:

    - Employees: BCMS Policy overview and what to do during or after a disruptive incident.
    - Customers: Business continuity measures taken, recent exercise and testing results, and how to contact the organization during a disruptive incident.
    - Local community: Business continuity measures taken and procedures for communicating with the organization during a disruptive incident.

4. **Create an Awareness Plan:** The awareness plan should inform employees and business partners regarding their role in the business continuity planning effort, with special emphasis on the policy, planning responsibilities, and where to go and what to do at the onset of a disruptive incident.

5. **Implement Document Management:** Document versioning, retention, and disposal processes ensure the most appropriate documentation is available to describe the planning process, as well as

support response/recovery to disruptive incidents. Many organizations will use a document revision table on official documentation to help identify the latest versions of documents, what changes were made to previous versions, and the person that approved the version. Regardless of the method used, the objective is to create an approach that ensures out-of-date versions of documents are not used, as this could cause confusion or a failure to appropriately respond to a disruptive incident.

BEFORE MOVING ON TO "OPERATION"

Allocating the necessary resources to the BCMS will ensure that the organization's business continuity objectives can be achieved. The resources addressed in Clause 7 illustrate a dedication to the BCMS and create the support needed to perform business continuity planning activities described in Clause 8.

As you continue reading this white paper, please note that we structured our description of Clause 8 differently than the way we described the other Clauses. Since Clause 8 represents the "Do" phase of the PDCA model and is highly descriptive, "Tips on Getting Started" are included under the individual sub-sections:

- 8.2 – Business Impact Analysis & Risk Assessment
- 8.3 – Business Continuity Strategy
- 8.4 – Business Continuity Procedures
- 8.5 – Exercising & Testing

ISO 22301 – CLAUSE 8 – OPERATION

PLAN DO CHECK ACT

WHAT IS IT?

ISO 22301 Clause 8 is the "Do" phase of the PDCA model (everything before it addresses the design and setup of the management system). Clause 8 is what many business continuity professionals consider the business continuity lifecycle – it is all about implementing the business continuity planning process for each element of the organization within the scope of the planning effort. Clause 8 describes the activities that should be performed to meet management's expectations. Key activities include:

Before discussing each element of Clause 8, Avalution would like to remind everyone that ISO 22301 is a "requirements" standard, meaning it describes what should be done, not how to do it. Guidance standards, such as ISO 22313 and other publications, summarize recommendations regarding how to perform activities, such as a Business Impact Analysis (BIA). Overall, the relatively low level of detail in Clause 8 is intentional and written to articulate what key elements make up a business continuity planning process.

WHAT VALUE CAN IT DELIVER?

Clause 8 describes the necessary performance of the business continuity planning lifecycle. It is here where those involved in preparedness work to minimize the likelihood of and impact associated with downtime, thus protecting the organization and its interested parties.

8.2 – THE BUSINESS IMPACT ANALYSIS AND RISK ASSESSMENT

As a business continuity management system standard, ISO 22301 describes the key elements of a BIA and risk assessment. In terms of outputs, the BIA enables the organization to:

- Identify the processes and activities necessary to deliver in-scope products and services
- Identify the resources necessary to deliver these processes and services
- Recommend recovery objectives for activities and resources (in line with management-approved downtime tolerances for products and services, but also with an understanding of potential costs associated with reaching these recovery objectives)
- Justify activity and resource recovery objectives, based on the potential impact of disruption

The risk assessment enables the organization to:

- Assess the likelihood of disruption to the activities and resources that deliver in-scope products and services based on a review of controls designed to "protect" key resources, including facilities, personnel, equipment, information technology, data, and suppliers/business partners
- Identify the potential causes or sources of disruption (commonly called threats)
- Recommend controls to limit the likelihood or impact of disruption to processes, activities, and resources (with an understanding of potential risk treatment costs)

ISO 22301 Clause 8.2.1 requires that an organization "establish, implement and maintain a formal and documented process for business impact analysis and risk assessment." A one-size-fits-all approach for both the BIA and risk assessment does not exist. However, at a minimum, ISO 22301 requires the identification of a formal, documented, value-adding process that can serve as a repeatable structure for conducting BIA and risk assessment efforts on a periodic basis, as well as identifying recommendations for improving the process in subsequent efforts. The BIA and risk assessment must have a defined output that aligns with the spirit and intent of the standard, including how frequently the information is to be updated and that the information is to be kept confidential. The standard also requires consistent criteria to reach BIA and risk assessment conclusions for those elements of the organization within the scope of the BCMS. Each of these points should be considered before defining and executing either the BIA or the risk assessment.

TIPS ON GETTING STARTED – BUSINESS IMPACT ANALYSIS

To align with the requirements noted in Clause 8.2.2 of ISO 22301, Avalution recommends following this three-step process:

1. Since the objective of the BIA is to assess or estimate the impact of disrupting the activities and resources necessary to create or deliver products or services, begin with a scoping effort that maps activities to the in-scope products or services that they create, deliver, or directly support.

2. For each of the activities and resources identified in the scoping effort, consider using an interview-based approach to collect the information necessary to enable the organization to reach appropriate conclusions, as this enables real-time discussion, follow-up questions, and an ability to hear the thoughts and justification that go into proposed objectives. The data gathering effort should include collecting:

    - Activity dependencies, including necessary resources;
    - Timeframe and resources required to resume operations after a disruption; and
    - Financial, operational, legal, regulatory, and reputational impacts of downtime to the organization, and how these impacts change over time.

3. Based on the information gathered from the interviews, determine how long each activity can be non-functional following the onset of a disruptive incident before the losses become unacceptable.

TIPS ON GETTING STARTED – RISK ASSESSMENT

To align with the requirements outlined in Clause 8.2.3 of ISO 22301, Avalution recommends following this four-step process:

1. Identify a risk assessment approach that meets the spirit and intent of ISO 22301. Review ISO 31000 and discuss other risk assessment approaches that may be in use throughout the organization (talk to internal audit, information security, and/or risk management).

2. Since the objective of the risk assessment is to identify the likelihood of a disruption to the processes and activities necessary to create or deliver a product or service, identify and describe the risk associated with specific disruptions. For example:

    - The risk of Process X downtime due to facility inaccessibility or loss
    - The risk of Process X downtime associated with the loss of staffing
    - The risk of Process X downtime due to the loss of Application X
    - The risk of Process X downtime due to the loss of Supplier X
    - The risk of Process X downtime due to the loss of Equipment X

3. Identify the potential sources or causes of a disruptive incident, including the likelihood of that disruption occurring. Consider the sources that impact the activity directly, such as a disruption that prevents the use of resources needed by the activity.

4. Identify potential options (controls) that reduce the likelihood of the risk.

CONCLUSIONS REGARDING "BUSINESS IMPACT ANALYSIS AND RISK ASSESSMENT"

When done correctly, the BIA and Risk Assessment establish the requirements that the organization should meet and risks that should be mitigated to align to management downtime expectations. Pragmatic, realistic risk mitigation opportunities and recovery objectives are the key outputs and serve as inputs into the development of business continuity strategies. Open for revision if strategies become cost-prohibitive, these outcomes establish the framework to move forward in the business continuity planning lifecycle as described in Clause 8.

8.3 – BUSINESS CONTINUITY STRATEGY

Following the completion of the BIA and risk assessment, it is important to assess what strategies may enable closure of the gaps or risks identified throughout these efforts, and provide a list of recommended risk treatments to enable risk mitigation, response, and recovery. Business continuity strategy essentially means the development of options and the selection of the most appropriate strategies that allow the organization to align with requirements. Key elements include:

- Identifying proactive measures to reduce the likelihood that a disruption occurs
- Identifying strategies that minimize the negative impact if a disruption were to occur
- Addressing stabilizing activities following the onset of a disruption, including incident response and recovery
- Listing resource needs that must be acquired to enable effective execution of strategies

Consistent with the intent of this standard, strategy selection also addresses third-party suppliers and business partners. Clause 8.3.1 clearly states, "The organization shall conduct evaluations of the business continuity capabilities of suppliers." As an extension of the risk assessment, the organization should evaluate supplier business continuity capabilities. Where gaps exist when compared to internal requirements (or ISO 22301), the organization should work with the supplier to improve its own business continuity processes and outcomes, or identify contingent supplier relationships (as warranted).

TIPS ON GETTING STARTED – BUSINESS CONTINUITY STRATEGY

To align with the requirements outlines in Clause 8.3 of ISO 22301, Avalution recommends following this three-step process:

1. Identify possible business continuity strategies that will reduce the risk identified in the BIA and risk assessment to levels that management finds acceptable. Three categories of business continuity strategy must be addressed:

    - Risk Mitigation
        - Identify opportunities to reduce the likelihood of a disruption, as well as strategies to limit the impact should a disruption occur. For example, consider implementing back up power generation to address the concern about a loss of commercial power at a critical facility.
    - Incident Response
        - Define the incident response process via threat-independent procedures, charter a team (with primary and alternate personnel) that will be charged with leading the response to a disruptive event, and identify the methods by which the team will activate, meet, assess the situation, and make decisions.
    - Recovery of Activities and Resources
        - Identify alternate sources of resources or alternate methods of performing required activities in order to meet downtime tolerances and obligations (alternate facilities, personnel, equipment, information technologies, and even third-parties, as well as manual workarounds if resources such as applications are unavailable).

2. Determine the resources necessary to implement each of the business continuity strategy categories.

    - Estimate the cost associated with implementing and maintaining the strategy.
    - Include all resources identified in the BIA that are required at the time of a disruption, including (but not limited to) people, information and data, facilities, transportation, and partners/suppliers.
    - Where appropriate, consider multiple strategy options (with pros, cons, and cost estimates) for addressing each risk. This approach enables management to measure investment requirements against organizational risk appetite to select the most appropriate strategy.

3. Submit the business continuity strategy options and recommendations to management for feedback, selection, and approval. With the information provided, management can evaluate the cost benefit analysis to determine the optimal strategies, based on requirements and the organization's risk appetite.

CONCLUSIONS REGARDING "BUSINESS CONTINUITY STRATEGY"

Business continuity professionals identify business continuity strategies to reduce risk in line with organizational requirements, including cost constraints, environment, obligations, risk appetite, and recovery objectives. By considering a broad range of risk treatment options, management can select the best options to arrive at an effective business continuity strategy. Once a business continuity strategy is selected, the business continuity professional should have the necessary support and resources to implement the selected strategy and develop business continuity procedures.

8.4 – BUSINESS CONTINUITY PROCEDURES

Developing business continuity procedures is what most business continuity professionals know as the "Planning" phase of the business continuity lifecycle. Business continuity procedures are the specific steps that the organization executes to respond, recover, and operate in "recovery mode" following the onset of a disruptive incident. ISO 22301 requires the development of business continuity procedures that:

- Detail specific steps to take immediately following a disruption that are flexible enough to adapt to an unanticipated incident and a changing situation
- Describe the incident response structure used in responding to a disruptive incident
- Describe the method used to monitor for an incident and alert stakeholders
- Enable activity and resource recovery

The incident response structure clearly describes the specific authorities and responsibilities for members of the response team. The incident response structure includes:

- Criteria for initiating a formal response to a disruption including key impact thresholds
- A clear management structure for decision making and additional authorities granted to the response team
- The resources allocated to the response team during a disruption

Further, ISO 22301 requires that the business continuity program formalize warning and communication procedures to identify a disruptive incident and communicate during a disruption. Required warning and communications procedures must address:

- Facilitating communication with first responders
- Identifying procedures to predict or identify a disruption, and then monitor and track the progress of the response
- Receiving communications from stakeholders and sending communications to stakeholders

In terms of plans – response and recovery – ISO 22301 Clause 8.4.4 requires content that:

- Helps the organization respond to a disruptive incident and meet recovery objectives
- Addresses initiating the response, executing recovery efforts and return to normal operations
- Describes the purpose and scope of the plan
- Describes the applicable recovery objectives
- Lists the criteria for activating the plan
- Documents clear roles and responsibilities for personnel involved in the response and recovery effort

There is not a single approach that all organizations can use to develop and document business continuity procedures. Clause 8.4.1 requires that organizations "establish, implement, and maintain business continuity procedures to manage a disruptive incident and continue its activities based on recovery objectives identified in the business impact analysis." The end goal should be to create a response structure, warning and communication procedures, and recovery plans that result in a repeatable, effective response and recovery process that can be invoked and executed without delay following the onset of a disruptive incident.

TIPS ON GETTING STARTED – BUSINESS CONTINUITY PROCEDURES

To align with the requirements noted in Clause 8.4 of ISO 22301, Avalution recommends following this four-step process:

1. Create a response structure that will facilitate a coordinated, effective, and efficient response to any disruption. To achieve this goal, the response structure should provide clear criteria for invoking the response and/or recovery effort and the decisions that the response team should consider making. Larger organizations may require response teams that coordinate distributed recovery efforts.

2. Determine who will be responsible for creating and updating each plan based on approved BIA-derived requirements and business continuity strategies.

3. Generate a structure for each plan owner to use in creating individual response and recovery plans. By creating a basic structure for the plan owners to use, the organization can ensure that all necessary information is included in the plans and reduce the effort required of plan owners. Detailed plan requirements are listed in Clause 8.4.4.

4. Work with the plan owners to generate the response and recovery plans for the organization. If the plan owners responsible for developing the plans have little to no experience in business continuity, then business continuity professionals should be prepared to assist plan owners in developing plan content in a collaborative manner so they meet the requirements set by the organization.

CONCLUSIONS REGARDING "BUSINESS CONTINUITY PROCEDURES"

When business continuity procedures are created correctly, the organization is able to respond to and recover from a disruption within the timeframe set by management. An effective response structure provides clear authority to individuals and teams involved in responding to a disruption, including where to go for assistance when a disruption meets escalation criteria. Warning and communications procedures ensure that the appropriate message reaches the intended audience without delay. Recovery plans detail a clear set of steps and resources needed to successfully recover from a disruption and restore operations to an acceptable level. Once the organization creates business continuity procedures, it is well-positioned to build response and recovery competencies and evaluate the adequacy of the procedures through exercises and tests.

8.5 – EXERCISING AND TESTING

The foundation of a strong business continuity management system is a focus on continual improvement. Exercising and testing business continuity strategies and procedures enables the organization to validate its capabilities in effectively responding to and recovering from a disruptive incident in the timeframe established by management.

Clause 8.5 requires an organization "exercise and test its business continuity procedures to ensure that they are consistent with its business continuity objectives." While there are myriad methods to implement exercises and tests, each organization's efforts should:

- Align to the scope and objectives of the BCMS
- Validate the effectiveness of the entirety of its business continuity strategies and procedures
- Ensure exercises and tests minimize disruption to normal operations
- Use realistic scenarios and clearly defined objectives
- Produce formalized reports that summarize the results of the exercise or test and include recommendations for continual improvement
- Conduct exercises regularly and when a significant change in the organization or environment occurs

ISO Technical Committee 223, the authors of ISO 22301, developed a separate guidance standard specifically focused on exercises (ISO 22398). Additional exercise-related planning, execution, and reporting-related detail may be found in that document.

TIPS ON GETTING STARTED – EXERCISING AND TESTING

To align with the requirements outlined in Clause 8.5 of ISO 22301, Avalution recommends following this three-step process:

1. Successfully exercising or testing business continuity strategies and procedures requires effective planning. To start, document the scope, objectives, assumptions, success and failure criteria, timeline, and list of participants. It's important to confirm that the exercise plan aligns to the organization's BCMS and that it will validate the entire BCMS scope when all exercises and tests are completed. Next, select the appropriate exercise type that will best validate the objectives for the defined scope, and then select an appropriate scenario that helps drive realism. Scenarios may focus on a loss of a resource (e.g. facility, technology, personnel) or be hazard-specific (e.g. hurricane) depending on scope and objectives established in the exercise and test plan.

2. Following development, facilitate the planned exercise. The complexity of the exercise or test will vary based on the type selected in the plan. Exercises or tests could be as simple as walking through the in-scope recovery plan step by step or as complex as conducting a full blown simulation that includes testing actual recovery resources. Although the facilitator can be internal to the organization (such as a business continuity professional) or external (such as a consultant), it's important that they possess these key traits:

    - Excellent presentation skills
    - Proven leadership abilities and comfort with the chosen exercise format
    - Knowledge of the organization and/or industry
    - Understanding of business and location-specific risks
    - Sufficient experience with the organization's business continuity program, especially the elements being exercised

3. Following exercise completion, capture all participant feedback regarding how the exercise met objectives, if the format of the exercise was best suited to meeting the objectives, and recommendations for improving the business continuity strategies and procedures (as well as the planning process). This feedback is critical, as it enables the identification of lessons learned and gap closure. Summarize the feedback and include in a final report for management's review and

feedback. Add any identified areas of improvement to a list of corrective actions (which will be discussed in Clause 10).

CONCLUSIONS REGARDING "EXERCISING AND TESTING"

Short of an actual disruptive incident, exercises and tests are the only way to validate business continuity and IT disaster recovery plan content and ensure that identified strategies are capable of providing response and recovery results within the timeframes approved by management. And, in addition to providing critical training to the personnel responsible for the response and recovery activities, exercising also helps pinpoint plan weaknesses, areas for improvement, and areas where business continuity and IT disaster recovery arrangements have become dated (and potentially ineffective). Ultimately, this element of Clause 8 is critically important as a means of demonstrating an appropriate level of performance.

BEFORE MOVING ON TO "PERFORMANCE EVALUATION"

The activities described in Clause 8 are usually performed annually, but may occur more frequently for higher priority products or services or when significant changes occur in the organization or environment. Clauses 9 and 10 help to identify improvement opportunities for the activities described in Clause 8, as well as the resulting outcomes. Before moving on to Clause 9, there is one important point we want to address. In the introduction of Clause 8, the following statement is made:

"The organization shall ensure that outsourced processes are controlled."

Avalution interprets this statement to mean that business continuity planning applies to all processes and resources owned and operated by the organization, as well as those processes and resources operated by others on behalf of the organization. As such, all of Clause 8 applies to both internal and outsourced operations that align to the scope of the BCMS.

ISO 22301 – CLAUSE 9 – PERFORMANCE EVALUATION

PLAN DO CHECK ACT

WHAT IS IT?

Performance evaluation serves as the "Check" phase of the PDCA model. The performance evaluation assesses the alignment of the BCMS (the operations of the BCMS, meaning clauses 4 through 7, as well as the planning process described in Clause 8) to management requirements and the requirements listed in ISO 22301. Clause 9 includes three key performance evaluation-related requirements, specifically:

- Establish, monitor, analyze and evaluate, and update metrics to assess performance of the BCMS at regular intervals
- Establish and maintain an internal audit process to ensure the BCMS aligns to management expectations and ISO 22301
- Communicate the performance of the BCMS and its solutions to program sponsors and other top management representatives through the management review process, with the objective of prioritizing continual improvement opportunities

The performance evaluation process is important because it allows the business continuity professional to convey the performance of the BCMS (both the management system itself, as well as the performance of business continuity solutions) to management without jargon. A well-executed performance evaluation will result in strong management feedback and help drive the implementation of corrective actions, thus improving and better aligning the BCMS to the organization's needs.

WHAT VALUE CAN IT DELIVER?

Independent feedback derived from metrics and an "internal audit" provides transparency and the input management needs to prioritize continual improvement opportunities. When done in a manner that assesses alignment to BCMS scope and objectives, management understands where gaps lie. Additionally, a high performing management review process keeps management interested and engaged, which is a key success factor for long-term performance.

TIPS ON GETTING STARTED

To align with the requirements outlined in Clause 9 of ISO 22301, Avalution recommends following this four-step process:

1. **Establish Measures and Metrics:** Metrics assess the ability of the BCMS to meet the requirements (such as downtime tolerance) established by management. The measures and metrics used to evaluate the performance of the BCMS should align to the requirements established in earlier phases of the BCMS and communicate performance in terms that management can easily understand. When defining metrics, do not communicate the number of BIAs and plans. Rather, communicate how product and service downtime tolerance compares to the actual recovery of activities and resources, how the BCMS performs based on the scope and objectives set by management, and

where gaps may exist. Prepare to summarize the business risk associated with gaps and poorly performing solutions.

2. **Implement an Internal Audit Process:** If one does not already exist, implement an internal audit process that can objectively evaluate the performance of the BCMS. Internal audit does not necessarily mean the internal audit department – after all, many organizations do not have such groups. Instead, it means having a qualified, independent person or group compare the BCMS (processes and solutions) to management expectations (as well as ISO 22301 if the organization seeks alignment). Create an internal audit work program and use it for recurring audits, and then take the results to measure continual improvement.

3. **Perform Management Reviews:** Use feedback from the metrics and internal audit (as well as other sources such as post-incident reviews, exercises, and other performance evaluations) to report readiness and alignment to management through the management review process. This is one of the most important and powerful aspects of the management system framework, as it enables the business continuity planning effort to stay connected with management. Define a consistent management review meeting agenda (using inputs from ISO 22301), but retain flexibility by incorporating special topics that require input from management. Make sure the management review is a two-way dialogue and keep it strategic, summarizing risk in terms management understands so that they can provide feedback. Management reviews may be needed more frequently early on in the design and implementation of a BCMS – perhaps monthly – and less frequently as the BCMS matures. Avalution does not recommend going more than three months without a management review of some form.

4. **Identify and Track Corrective Actions:** Based on management's feedback, prepare to develop or refine corrective actions to drive continual improvement for remediation (see Clause 10). Prepare to report the status of corrective action closures during periodic management reviews.

BEFORE MOVING ON TO "IMPROVEMENT"

Clause 10 – Improvement is not possible without the requirements noted in Clause 9. Do not be afraid to collect performance-related feedback and communicate it in an efficient manner to your program sponsor and other management representatives. Explaining the "goods and the bads" is important so they know where to apply limited resources to protect the organization.

ISO 22301 – CLAUSE 10 – IMPROVEMENT

PLAN DO CHECK ACT

WHAT IS IT?

Clause 10, the BCMS' improvement process, is the "Act" phase of the PDCA model. The objective of the improvement process is to enable the program to close gaps to more closely align to management expectations and organizational obligations. ISO 22301 requires that the organization identify nonconformities, determine the cause(s) so as to avoid recurring poor performance, and implement corrective actions as necessary.

WHAT VALUE CAN IT DELIVER?

Most business continuity professionals facilitate activities to identify improvement opportunities, but far fewer implement a process to prioritize, manage, and report on progress toward closure of these improvement opportunities. The primary focus of Clause 10 is to get organized and enable the prioritized closure tracking of continual improvement opportunities by focusing limited resources on the feedback that drives performance.

TIPS ON GETTING STARTED

To align with the requirements outlined in Clause 10 of ISO 22301, Avalution recommends following this three-step process:

1. **Corrective Actions:** Define a process and repository to manage corrective actions. This process could be as simple as a spreadsheet or SharePoint list. The corrective action list (or database) should track the progress of implementing and closing corrective actions. The corrective actions repository should include the following information, customized based on the unique needs of the organization:

COLUMN NAME	DESCRIPTION
Creation Date	Enter the date the corrective action item was added to the repository.
Corrective Action Title	Identify the title of the corrective action.
Description	Describe the issue, highlighting root cause and possible remediation action.
Source of Corrective Action	Identify the source of this improvement opportunity.
Priority	Identify the priority of this corrective action.
Status	Identify the status of this corrective action.
Initial Date	Identify the date the corrective action was either identified or entered into the repository.
Due Date	Identify the date this corrective action is due to be resolved.
Responsible Individual	Select the person responsible for this corrective action.

Actual Resolution Date	Identify the date this corrective action was resolved.
Comments	Additional comments on the corrective action.

2. **Root Cause Analysis:** Perform a root cause analysis of how and why the issue occurred. A root cause analysis is a process to understand why a performance issue occurred and address the reason so as to avoid a reoccurrence. ISO 22301, unlike previous standards, notes the need to perform a root cause analysis (which does not have to be complex process).

3. **Reporting:** Periodically, check the progress of outstanding corrective actions, as well as any deviation from the expected timeframe and milestones, and report the progress and status to management via the management review process.

CONCLUSIONS

The publication of ISO 22301 resulted in the first international standard that summarizes business continuity best practices applicable to all organizations. Written using language that anyone can understand, ISO 22301 is designed first and foremost to drive business continuity performance, and if a business case exists, organizational certification.

As discussed throughout this white paper, the standard was not written to make someone an expert in business continuity, nor was it written as a "how-to" guide. Rather, it summarizes what an international group of business continuity experts feel are the key elements of a business continuity management system to ensure readiness for a wide-variety of disruptive incidents. Additionally, ISO 22301 is what many professionals call an umbrella standard, meaning it can help organize alignment with and incorporate other standards, such as those focused more deeply on sub-disciplines, such as IT disaster recovery, or perhaps even something more strategic, such as risk management in general.

NEXT STEPS

Avalution has been a longtime proponent of aligning to standards, and, if a business case exists, proceeding toward organizational certification. We encourage you to review the resources provided throughout this white paper and invite you to reach out to us if you have questions regarding the implementation of ISO 22301 or business continuity management systems in general, as our team always welcomes a conversation about how certification or alignment to a standard can benefit your organization.

I WOULD LIKE TO DISCUSS:
ALIGNING TO ISO 22301

I WOULD LIKE TO DISCUSS:
ISO 22301 CERTIFICATION

ABOUT AVALUTION CONSULTING

Avalution Consulting – the 2012 BCI North America Business Continuity/Disaster Recovery Company of the Year – specializes in business continuity and IT disaster recovery consulting, outsourcing, and software solutions for organizations in both the public and private sectors. Avalution also assists in preparing organizations for ISO 22301 certification, as well as assessing readiness for the certification process. Headquartered in Cleveland, Ohio (USA), Avalution is an ISO 22301 certified firm and maintains a contract on GSA Schedule 70. In addition to consulting services, Avalution offers two unique, web-based business continuity software solutions:

Catalyst business continuity software combines a simple user interface and on-screen guides with Avalution's industry-leading methodology to make continuity planning easy and repeatable for every organization, regardless of size, industry, or geography. Features include policy and procedure development, business impact analysis, risk assessment, recovery strategy definition, plan development (business and IT), exercising, live incident management, and emergency notification. No long-term contracts are required, and a 30-day free trial is available via the website.

The Planning Portal – an enterprise level solution based on the simplicity of Microsoft SharePoint 2010 – delivers highly customizable tools and processes to assist in managing and executing business continuity and IT disaster recovery programs. Solutions address analysis, planning, awareness generation, exercise planning, notification, live crisis management, and continuous improvement. Demonstrations are available upon request.

866.533.0575 | avalution.com | theplanningportal.com | bccatalyst.com | Follow Us: