

A Maturity Model for the Phased Implementation of the ANSI/ASIS.SPC.1:2009 Organizational Resilience Standard

Dr. Marc Siegel, ASIS International

Maya Siegel, Brandeis University

Introduction

Implementation of a management system standard can be a daunting task, especially for small to medium sized enterprises (SMEs). All organizations face the challenge of managing their risks within the bounds of organizational objectives and available resources. Through the full implementation, ongoing maintenance and continual improvement of the ANSI/ASIS.SPC.1:2009 Organizational Resilience Management System an organization is able to reach ultimate goal of assuring organizational resilience. The phased approach recognizes that resilience must be achieved in balance with the business needs of the organizations and its time and financial constraints by building a system that is continually improving, growing and maturing.

Success breeds success. A maturity model for the phased implementation of the ANSI/ASIS.SPC.1:2009 Organizational Resilience Standard provides several advantages. By selecting initial projects to demonstrate the benefits of the ANSI/ASIS.SPC.1 management system, it is possible to build and maintain the support and commitment of the stakeholders, staff and management. Building the system in a phased approach and achieving benchmarks of maturity, provides the organization a link between costs and value added. It provides a basis for managing risk and resilience while reducing costs, demonstrating legal and regulatory compliance, enhancing stakeholder relations, and meeting customer and supply chain expectations.

Organizations may have different reasons for pursuing the implementation of the ANSI/ASIS.SPC.1, from addressing identified problems, to exploiting opportunities for improvement, to gaining business advantage. All organizations benefit from enhanced organizational resilience. The maturity model for phased implementation places the focus on the continual improvement of the systems approach for resilience management. The aim is to become more resilient and to better manage the organization's risks. The maturity model provides achievable steps tailored to the economic and temporal realities in which the organization must operate. The organization can expand and improve its resilience management system consistent with the context in which it operates, the objectives of the organization, and the availability of resources.

The maturity model does not assume an organization will seek third-party certification. Rather, the approach outlined in this paper assumes that the driving force for pursuing the implementation of the ANSI/ASIS.SPC.1:2009 Organizational Resilience Standard is to establish a management system for the continual improvement of resilience performance. Therefore, the model should not be viewed as a certification instrument but rather a tool to help organizations become better educated

and aware of the benefits of resilience management and preparedness. The tools in the standard help organizations phase in a management system timed to their business needs and economic realities. The approach defined in the standard can be used by any organization, regardless of whether they will eventually make a business decision to seek first, second, or third-party validation of their conformance with the requirements of the ANSI/ASIS.SPC.1:2009 Organizational Resilience Standard.

Promoting a Culture of Resilience Management and Preparedness

All organizations face a certain amount of uncertainty and risk. Organizations must have a system to manage their risks in order assure sustainability of operations and maintain resilience, competitiveness and performance. The challenge is to determine how much risk and uncertainty is acceptable and how to cost effectively manage that risk and uncertainty while meeting the organization's strategic and operational objectives. Given the finite resources of organizations, it is imperative that they have business-friendly tools to address an array of threats, hazards and risks they may face.

For a resilience management and preparedness program to be effective, it must be implemented by every person within the organization. For this to occur a significant culture paradigm shift is required, where managing risks is no longer seen as just the responsibility of management. The risk makers and the risk takers must also be the risk managers. Everyone within the organization must take ownership of the process, making resilience management and preparedness an integral part of the culture of the organisation. Implementation of a management system is both by and for the organization, and should be fully integrated into all aspects of the organization. Therefore, the implementation approach needs to generate excitement and garner support throughout all levels within the organization through selling the vision of the benefits derived from resilience management and preparedness.

A maturity model for the phased implementation of the ANSI/ASIS.SPC.1:2009 helps develop the momentum in support of the resilience management and preparedness needed to encourage persons to manage their risks by seeing clear benefits of their participation. By carefully setting objectives and targets to maximize chances of early success, it is possible to stimulate top management support and acquire the needed resources to implement the management system. Publicizing and recognizing success breeds the necessary levels of enthusiasm and credibility throughout the organization to move from phase to phase towards the goal of a fully integrated resilience management and preparedness system.

Maturity Model for the Phased Implementation of the ANSI/ASIS.SPC.1:2009

This model outlines six phases of implementation of the ANSI/ASIS.SPC.1:2009 ranging from no process in place for resilience management to going beyond the requirements of the ANSI/ASIS.SPC.1:2009 to considering the organization's role in community and supply chain

resilience. The goal is to achieve total integration of resilience management in all the organization's everyday activities and functions. In other words, the goal of this maturity model is to establish a resilience management and preparedness culture throughout the organization.

The maturity model, for the phased implementation of the ANSI/ASIS.SPC.1:2009, is a series of steps designed to help organizations evaluate where they currently are with regard to resilience management and preparedness, to set goals for where they want to go, to benchmark where they are relative to those goals, and to plot a business sensible path to get there. Standards are designed to promote managed and repeatable performance. This will be achieved by moving up the phases of the model.

Phase One: Ad Hoc Approach

This is the pre-awareness phase where the organization is not conducting pre-planning but rather reacting to situations as they arise in an ad-hoc fashion. No formal incident or resilience management process is currently in place. The key barrier in this phase is a lack of information and knowledge about resilience management. Resilience management and preparedness are frequently seen as a financial burden on an organization without a clear benefit to proactive planning. Management is ambivalent or anxious that the recognition of problems is an admission of weakness. Comfort is sought in the assumption that by not identifying or recognizing problems the organization is not accountable for the problems.

In order to move from Phase One to Phase Two, the organization needs to recognize the need and the value of resilience management and preparedness. A disruptive event may trigger a realization within the organization that pre-planning might have saved the organization time and money. External factors, such as stakeholder concerns, contractual requirements, or government encouragement may cause the organization to consider exploring a more proactive approach. Once the organization becomes aware of the potential benefits of resilience management, it is ready to move on to Phase Two.

Phase Two – Project Approach

The project approach is the awakening phase. Management is willing to test the concept and establish a trial project to explore the benefits of resilience management and preparedness. A limited scope project is established to address specific issues using the core elements of the standard as a guide for how to improve performance.

Management should clearly define the objectives and expectations of the project. Management then designates a "Project Leader" with the authority and competence to conduct the project and serve as the resilience champion. To assure the best outcome of the project, issues addressed must be carefully selected to maximize the likelihood of quick success. The project focus is on demonstrating the need and value of resilience management and preparedness. The underlying

assessment of the project is a gaps analysis; examining what is needed to achieve the goals of the project. This is in order to recognize and publicize a success to generate momentum for a broader resilience management and preparedness program.

Recognizing that this is a business project is critical to the success of this phase. Therefore, as with any business project it requires clear definitions of objectives, authorities, roles, responsibilities, budgets and timeframes, as well as a method to measure and monitor outcomes. To conduct the project successfully the Project Leader needs to have management support, including adequate resources. In addition, access to adequate training and expertise is needed to support the Project Leader and members of the project team are necessary.

The standard provides a structure for approaching and resolving the issues that need to be addressed. Implementation entails applying as many of the core elements of the standard as possible to improve resilience performance and preparedness relative to the identified elements. Attention is focused on addressing the “low hanging fruit” issues rather than emphasizing the management system framework structure. Based on the outcomes of Phase Two, the organization can decide whether to conduct Phase Three or go directly to Phase Four.

Phase Three – Program Approach

The program approach is an expansion of the project approach. The view shifts from specific issues to addressing division or organization wide issues implementing the core elements of the standard. Focus is placed on the activities outlined in the individual core elements rather than their interrelationships and integration of the elements. Risk management applications are selected for their chances of demonstrating success and awareness. In this phase, top management recognizes the importance of the elements and the need for pre-planning. The application of the standard is still in a pilot testing mode. Parts of the organization are applying the elements of the standard and testing action plans to make a business case for implementing the management system standard in full.

This phase provides the opportunity to increase awareness to a larger portion of the organization. The “Program Manager”, appointed and endorsed by top management, expands the project to address broader issues related to the organization’s reliability, sustainability and survivability in the event of a disruption. Emphasis is on developing a series of action plans to deal with critical issues. The issues selected may be in reaction to an incident or near miss, or be driven by external concerns. When developing the action plans the organization develops proactive plans to better respond to the identified issues. The organization should consider measures to reduce the likelihood of disruptive incidents and the consequences. Typically, more weight is given to proactive planning to address the symptoms and consequences of a disruption.

Phase Four – Systems Approach

Phase Four involves putting the pieces together. Core elements are flushed out with special attention paid to them rather than their interrelationships and the integration of the elements. The core elements are viewed in terms of identifying and addressing root causes of disruptions and creating economically viable solutions which address the root causes. Resilience management and preparedness are viewed as part of an iterative continual improvement process using the Plan-Do-Check-Act model. Integration and feedback loops of the systems approach encourage learning from experience.

In this phase, top management recognizes, understands and is committed to the strategic importance of resilience management and preparedness. Top management is actively engaged in the elements of the management system and standard. Critical business functions and activities have been identified, risk criteria set, and the risks are prioritized. The focus is on identifying opportunities for improvement in resilience and preparedness performance. Various parts of the organization are testing the standard's core elements to refine the implementation of the standard. Audit findings are used to identify opportunities for improvement in order to reinforce the competitive and strategic advantage of the organization. By the end of this phase, a culture of resilience and preparedness is clearly taking hold in the organization.

Phase Five – Management System

By this phase, the management system is now fully implemented consistently throughout the defined scope of the organization. The organization can now demonstrate conformance to the standard (either by first, second or third party validation). A multi-year perspective recognizing the utility of the management system standard has been visibly endorsed by top management, and resilience and preparedness are fully integrated into the organizations functions and activities. A resilience management culture is promoted within the organization encouraging persons throughout the organization to take ownership of risk and think about their role in identifying, assessing and managing risk to promote resilience and preparedness.

The managing of risk uses balanced strategies to adaptively, proactively and reactively address the minimization of both the likelihood and consequences of disruptive events. However, adaptive and proactive strategies are clearly seen as the preferred approaches to managing risks. Risk management, risk assessment and resilience management are considered key components of the overall decision-making process in the organization. Resilience, preparedness training, and awareness are routine parts of the human resource management of all persons providing services to the organization.

By now, all the core elements of the standard have been applied and tested. Audits, evaluations and management review moves beyond a focus on opportunities for improvement to promoting competitive advantage and extending the management systems approach to new applications,

divisions and parts of the enterprise. There is a continual drive to make the system processes more efficient and effective to support continued interest and excitement in the resilience management and preparedness processes.

Phase Six – Holistic Management

In phase six, the organization goes beyond conformance to the standard to fully integrate resilience management and preparedness into its overall risk management strategy. The organization emphasizes enterprise-wide and supply chain relationships, as well as community responsibilities, in all aspects of its resilience management system. Resilience management culture is well developed and is considered an inseparable part of decision making. Resilience management and systems principles are expanded to all areas of business and activities.

The organization mentors other stakeholders (in its supply chain and community) recognizing that organizational resilience is an integral part of community resilience.

Recognition Program

The maturity model can serve as the basis for a recognition program within the organization. Each stage represents a benchmark of performance and achievement. By using a recognition program, the organization can incentivize its stakeholders to continually improve resilience and preparedness performance. The maturity model establishes realistic achievable goals for the organization to maintain the level of performance within resource constraints.

Using a simple recognition structure, the stages can be translated into the following achievement levels:

- Phase One: Coal
- Phase Two: Bronze
- Phase Three: Silver
- Phase Four: Gold
- Phase Five: Platinum
- Phase Six: Diamond

Maturity Model Matrix

The following matrix outlines the perspectives and activities that should be considered for the different phases of implementation of the ANSI/ASIS.SPC.1. The matrix provides guidance on how an organization can structure a fit-for-purpose program to fit their organization's business needs and realities. Organizations can use this matrix as a basis for a recognition program to evaluate their level of performance.

Maturity Model for the Phased Implementation of the ANSI/ASIS.SPC.1:2009 Organizational Resilience Standard

ANSI/ASIS.SPC1 Standard Clause	Core Element	Issues Addressed by Core Element	Ad Hoc Approach Phase One	Project Approach Phase Two	Program Approach Phase Three	Systems Approach Phase Four	Management System Phase Five	Holistic Management Phase Six
Generic Concepts	Key elemental theme	Description of element	<ul style="list-style-type: none"> - No formal incident or resilience management - Actions are reactionary in nature - Not yet recognizing the importance of elements 	<ul style="list-style-type: none"> - Initiates a project to address specific issue(s) by partially implementing core elements - Actions generally reactionary in nature focusing on pre-identified issue(s). - Recognizes the importance of elements and the need for some pre-planning - May be in reaction to an incident or near miss or be driven by external concerns 	<ul style="list-style-type: none"> - Establishes a division or organization wide program to address resilience issues by partially implementing core elements - Recognizes the importance of elements and the need for pre-planning, however focus is on individual elements and not their interrelationship and integration - May be in reaction to an incident or near miss or be driven by external concerns - Risk management applications selected for their chances of demonstrating success - Program driven by "Program Manager" who applies a program management approach 	<ul style="list-style-type: none"> - Resilience management is viewed as a matter of strategic value to the organization - Focuses on integration and interrelationships between core elements - Focuses on proactive management of risks to minimize both likelihood and consequences of a disruptive incident - Resilience management is viewed as part of a continual improvement process using PDCA model - Managing risk is seen as important at all levels and roles in organization - Integration and feedback loops of systems approach ensures effective learning from experiences - Resilience management culture is developing and part of decision making 	<ul style="list-style-type: none"> - The organization is conformant with the requirements of the standard - The organization establishes, documents, implements, maintains, and continually improves an organization resilience management system in accordance with the requirements of the ORMS Standard, and determines how it will fulfill the requirements. - Examines the linkages and interactions between the elements that compose the entirety of the system - Manages risk using balanced strategies to adaptively, proactively and reactively address minimization of both likelihood and consequences of disruptive events - Resilience management becomes part of the routine management of projects and business processes 	<ul style="list-style-type: none"> - The organization goes beyond conformance to the standard to fully integrate resilience management into its overall risk management strategy - The organization emphasizes enterprise-wide and supply chain relationships in all aspects of its resilience management system. - The organization mentors other stakeholder (in its supply chain and community) recognizing that organizational resilience is an integral part of community resilience - Resilience management culture is well developed and considered a inseparable part of decision making - Resilience management and systems principles are expanded to all areas of business and activities

Maturity Model for the Phased Implementation of the ANSI/ASIS.SPC.1:2009 Organizational Resilience Standard

ANSI/ASIS.SPC1 Standard Clause	Core Element	Issues Addressed by Core Element	Ad Hoc Approach Phase One	Project Approach Phase Two	Program Approach Phase Three	Systems Approach Phase Four	Management System Phase Five	Holistic Management Phase Six
4.1.1 Scope of OR Management System	- Understands the organization and its context - Scope of ORMS	- Establishes the internal, external and risk management context of the organization - Defines scope and boundaries for development and implementation of ORMS.	- No formal process - No definition of scope or internal or external context - No clear concept of business context or benefits	- Projects of limited scope focusing on one or a limited number of issues identified as of particular or immediate interest - Internal and external context and interactions considered within project scope definition	- Programs are established to address core elements based on evaluation of the internal, external and resilience management context of all or part of the organization - Scope defined based on protecting and preserving critical activities, functions and services	- Organization defines and documents the internal, external and resilience management context - Critical operational objectives, assets, activities, functions, services, and products are defined - Boundaries of scope are defined and documented based on protecting and preserving critical activities, functions and services, as well as relations with stakeholders - Weighting of risk management strategies is defined	- Organization defines and documents the internal, external and resilience management context, as well as organization-wide risk management interactions - Boundaries of scope defined and documented considering the organization's mission, goals, internal and external obligations, and legal responsibilities	- Organization defines and documents the internal, external and resilience management context, as well as enterprise-wide risk management interactions and supply chain tier, commitments and relationships - Boundaries of scope defined and documented
4.2.1 Policy Statement	- Setting a policy framework	- Establishes a policy to provide a framework for setting objectives and provide the direction and principles for action. - Demonstrates management commitment	- No defined policy - Lack of top level governance	- Policy limited to addressing identified issue(s) - Driven by "Project Leader", may or may not have top management involvement beyond approval of project	- Drafted by "Program Manager" and signed by top management - Policy addresses resilience management in divisions defined in scope - Communicates to relevant divisions	- Policy establishes framework for resilience management by setting objectives and providing direction - Endorsed by top management - Communicated throughout organization	- Policy establishes framework for resilience management by setting objectives and providing direction - Clear commitment to comply with applicable legal and other requirements - Endorsed and promoted by top management - Communicated throughout organization and to stakeholders making them aware of content and meaning	- Policy establishes framework for internal and external resilience management by setting objectives and providing direction - Clear commitment to comply with applicable legal and other requirements - Endorsed and promoted by top management - Communicated throughout organization, enterprise and supply chain
4.2.2	- Management	-Demonstrates top	- Management	- Management	- Top management	- Top management	- Documents evidence	- Documents

Maturity Model for the Phased Implementation of the ANSI/ASIS.SPC.1:2009 Organizational Resilience Standard

ANSI/ASIS.SPC1 Standard Clause	Core Element	Issues Addressed by Core Element	Ad Hoc Approach Phase One	Project Approach Phase Two	Program Approach Phase Three	Systems Approach Phase Four	Management System Phase Five	Holistic Management Phase Six
Management Commitment	mandate and commitment	management and the organization's commitment to meeting the requirements of resilience management. - Establishes the project to address resilience management including the provision of appropriate resources and authorities for conduct project.	ambivalent to unreceptive - Concerned that acknowledging risk and uncertainty may be seen of admission of problems or weakness - No guidance from the top or organization - Ad hoc leadership - Ostrich effect	authorization and resources provided to "Project Leader" to conduct project including in-house training and/or external expertise - Resources restricted to address limited scope. - Resource allocation linked to perceived return on investment - Project aims to encourage more management support and buy-in	sponsorship - Endorsement of established programs for resilience management - One or more individuals appointed as Project Manager - Set asset prioritization and timeframes for recovery in event of disruption - Resources allocated to support program	participation - Visible endorsement of top management - Establishes an ORMS policy - One or more individuals appointed to be responsible for ORMS - Decides criteria for accepting risk, acceptable levels of risk - Sets asset prioritization and timeframes for recovery in event of disruption - Resources allocated to support system	of its mandate and commitment to the establishment, implementation, operation, monitoring, review, maintenance, and improvement of the ORMS - Defines and documents criteria to be used to evaluate the significance of risk, determination of appropriate risk treatments, and setting of timeframes for recovery - Sufficient resources allocated and competencies assured	evidence of its mandate and commitment to the establishment, implementation, operation, monitoring, review, maintenance, and improvement of the ORMS - Defines and documents criteria to be used to evaluate the significance of risk, determination of appropriate risk treatments, and setting of timeframes for recovery for the organization and relevant stakeholders
4.3.1 Risk Assessment and Impact Analysis	- Identification and valuation of asset, activities, functions and services - Risk identification - Risk Analysis - Risk Evaluation	- Establishes a process for risk identification, analysis and evaluation. - Identifies assets, activities, needs, requirements and analysis of critical issues related to business disruption risks that are relevant to the organization and stakeholders. - Identifies hazards threats, vulnerabilities and consequences. - Evaluates the effect of uncertainty on the organization's objectives. - Evaluates the likelihood of a disruptive event and its consequences on assets (human, physical, cyber, environmental, information, and	- No formal process - Indications of problems, near misses and warning signs identified in an ad hoc manner as they materialize - Risks are identified after they materialize	- No formal process - Reactive in nature with issue(s) addressed having been identified due to indications of problems, near misses, warning signs, an event, and/or external concerns - The analysis is more of a gap analysis than a risk assessment examining what is need to address project issues	- Develops and implements a procedure to identify, analyze and evaluate critical assets, risks, and impacts - Priorities based on outcomes of risk analysis or business impact analysis	- Establishes, implements, and maintains an ongoing formal and documented risk assessment process - Prioritizes risks and their impacts are taken into account in establishing, implementing, and operating the ORMS - Risk assessment and impact analysis recognized as providing the foundation for elements of the ORMS and for organizational decision-making	- Establishes, implements, and maintains an ongoing formal and documented risk assessment process - Prioritizes risks and their impacts are taken into account in establishing, implementing, and operating the ORMS - Periodically reviews whether OR management scope, policy, and risk assessment are still appropriate given the organizations' internal and external context - Re-evaluates risk and impacts within the context of changes within the organization or made to the organization's operating environment,	- Establishes, implements, and maintains an ongoing formal and documented risk assessment process - Establishes, implements, and maintains a formal and documented communication and consultation process with stakeholders and supply chain partners in the risk assessment process - Establishes, implements, and maintains a formal and documented process for monitoring and reviewing the risk

Maturity Model for the Phased Implementation of the ANSI/ASIS.SPC.1:2009 Organizational Resilience Standard

ANSI/ASIS.SPC1 Standard Clause	Core Element	Issues Addressed by Core Element	Ad Hoc Approach Phase One	Project Approach Phase Two	Program Approach Phase Three	Systems Approach Phase Four	Management System Phase Five	Holistic Management Phase Six
		intangible). - Evaluates dependencies and interdependencies with other assets and sectors, and consequences a disruptive event. - Evaluates and establishes timeframes for response and recovery.					procedures, functions, services, partnerships, and supply chains	assessment process
4.3.2 Legal and Other Requirements	- Identifies legal, regulatory, and other requirements to which the organization subscribes - Determines how these requirements apply to the organization, its risks and their potential impacts.	- Identifies legal and other requirements which govern the organization's activity. - Establishes a procedure or process for identifying, registering and evaluating internal and external requirements pertinent to the organization's functions, activities and operations. - Understands and communicates the potential impact of laws, regulations, codes, zoning, standards or practices concerning emergency procedures specific to location and industry.	-No understanding of legal and other requirements	- Informal process initiated to identify legal and other requirements related to identified issue being addressed - The main legal requirements applicable to the activities, functions and services in the scope of the project are identified	- Identifies legal and other requirements	- Establishes and maintains procedures to identify legal and other requirements - Determines how the legal and other requirements apply to the organization - Communicates requirements to appropriate parties	- Establishes and maintains procedures to identify legal and other requirements - Determines how the legal and other requirements apply to the organization risks and obligations - Ensures that applicable legal, regulatory, and other requirements are considered in developing, implementing, and maintaining its organizational resilience management system - Documents information and keeps it up-to-date	- Establishes and maintains procedures to identify legal and other requirements relevant to the organization and appropriate stakeholders - Determines how the legal and other requirements apply to the organization and stakeholder risks and obligations
4.3.3 Objectives, Targets, and Program(s)	- Sets objectives and develops risk and incident prevention, protection, preparedness, mitigation, response, continuity and recovery management strategies - Risk prioritization and treatment	- Prioritizes the issues identified as a result of the risk assessment and impact analysis. - Sets objectives and targets (including time frames) based on the prioritization of issues within the context of an organization's policy and mission. - Develops strategic plans for incident prevention, protection, preparedness, mitigation, response,	- Objectives and targets not defined - No risk prioritization	- Defines targets and objectives based on the supporting demonstration of perceived factors for project success in dealing with identified issue(s) - Develops targets, objectives and programs to achieve immediate resilience	- Resilience performance objectives for program management are set based on the risk assessment and impact analysis - Strategic action plans designate actions, responsibilities, accountability, resources and timeframes for achieving objectives	- Objectives shall be derived from and are consistent with the OR management policy and risk assessment - Documents objectives and targets to manage risks in order to avoid, prevent, protect, deter, mitigate, respond to, and recover from disruptive	- Documented objectives and targets are established to manage resilience by avoiding, accepting, removing the source, changing the likelihood, changing the consequences, sharing and/or retaining the risk - Objectives provide a basis for selecting one or more options for modifying risks considering asset value, opportunities for reducing likelihood	- Documented objectives and targets establish internal and external expectations for the organization and its stakeholders that are critical to mission accomplishment, product and service delivery, and functional operations

Maturity Model for the Phased Implementation of the ANSI/ASIS.SPC.1:2009 Organizational Resilience Standard

ANSI/ASIS.SPC1 Standard Clause	Core Element	Issues Addressed by Core Element	Ad Hoc Approach Phase One	Project Approach Phase Two	Program Approach Phase Three	Systems Approach Phase Four	Management System Phase Five	Holistic Management Phase Six
		continuity and recovery. - Identifies the resources needed and the availability of adequate human, infrastructure, processing and financial resources. - Identifies roles, responsibilities, authorities and their interrelationships within the organization as far as needed to ensure effective and efficient operations. - Plans the operational processes for actions effecting how the objectives and targets are achieved. - Makes internal and external arrangements, agreements, and contingency plans that need to be in place to manage foreseeable emergencies.		performance improvement related to identified issue(s) and to demonstrate business benefit - Addresses issue(s) using rudimentary PDCA model approach focusing on limited scope - Action plans include actions necessary, required human and financial resources, responsibilities and timescales	and targets	incidents are established - Targets are measurable and derived from the objectives - Establishes and maintains one or more strategic programs (action plans) for prevention, protection, deterrence, mitigation, response, continuity and recovery - Strategic plans designate actions, responsibilities, accountability, resources and timeframes for achieving objectives and targets	and/or consequences, cost/benefit, and tolerable levels of residual risk - Targets are measurable, achievable, relevant and time-based - Establishes, implements and maintains one or more program(s) for risk treatment in order to achieve its objectives and targets - Risk treatment options (defined in action plans) consider the prevention, protection, deterrence, mitigation, respond, and recover from disruptive incidents. The programs shall be optimized and prioritized in order to control and treat risks associated with threats, hazards and impacts of disruptions to the organization and its stakeholders	
4.4.1 Resources, Roles, Responsibility, and Authority	- Ensures the availability of resources essential for the implementation and control of the ORMS. - Roles, responsibilities, and authorities shall be defined, documented, and communicated in order to facilitate effective OR management.	- Establishes procedures, roles and responsibilities to cover all normal and abnormal operating conditions, including disruptions and emergencies. - Establishes management processes and procedures for human resources including employees, contractors, temporary staff, etc. - Identifies and assures availability of human, infrastructure and financial resources in the event of a disruption. - Establishes and documents provisions	- Not defined - No dedicated personnel for resilience management - Needed resources not identified - Lack of time, energy and resources to adequately prepare for and respond to disruptions	- Assigns roles and responsibilities to specific persons to address issue(s) in the limited scope - Allocates adequate resources in accordance with action plan - A "Project Leader" is designated to oversee the conduct of the project - Participation based on project scope (only	- Identifies and defines authorities, roles, responsibilities and appropriate resources within the organization - Identifies internal and external departments, division, business units and partners that will pay a role in addressing a disruptive incident - Identifies an incident management team and team leader - Allocates adequate resources in accordance with the	- Top management appoints a specific management representative responsible for the ORMS - Formal resilience management responsibilities and relationships are defined and adhered to - Teams with defined roles and adequate resources are established to support resilience action plans - Establishes arrangements for	- Roles, responsibilities, and authorities are defined, documented, and communicated in order to facilitate effective organizational resilience management, consistent with the achievement of its organizational resilience management policy, objectives, targets and programs - Resilience, crisis, and response team(s) with defined roles, appropriate authority, and adequate resources to oversee incident management are established	- Roles, responsibilities, and authorities are defined, documented, and communicated in order to facilitate effective organizational resilience management within the organization, enterprise-wide and within the community consistent with achieving organization, stakeholder, supply chain and community

Maturity Model for the Phased Implementation of the ANSI/ASIS.SPC.1:2009 Organizational Resilience Standard

ANSI/ASIS.SPC1 Standard Clause	Core Element	Issues Addressed by Core Element	Ad Hoc Approach Phase One	Project Approach Phase Two	Program Approach Phase Three	Systems Approach Phase Four	Management System Phase Five	Holistic Management Phase Six
		for adequate finance and administrative resources and procedures to support the management program or system normal and abnormal conditions. - Makes arrangements for supply chain obligations, mutual aid and community assistance. - Determines the local, regional and public authorities' roles, relationships and interactions with the organization's management system implementation plans.		divisions and individuals within the scope actively engaged)	action plan	stakeholder assistance, communication, strategic alliances and mutual aid - Identifies financial and administrative procedures needed to support the resilience programs and meet objectives and targets - Roles, relationships and interactions with local regional and public authorities (including first responders) are defined - Adequate resources allocated in accordance with action plan	- Establishes logistical capabilities and procedures to locate, acquire, store, distribute, maintain, test, and account for services, personnel, resources, materials, and facilities produced or donated to support the organizational resilience management system - Establishes procedures for stakeholder assistance, communications, strategic alliances, and mutual aid	resilience objectives, targets and programs
4.4.2 Competence, Training, and Awareness	Awareness, competence and training strategies, plans, programs and procedures	- Identifies and establishes skills, competency requirements, and qualifications needed by the organization to maintain operations. - Assesses, develops and implements training/ and education program for the organization's personnel, contractors, and other relevant stakeholders. - Develops organizational awareness and establish a culture to support resilience management. - Determines organizational interface protocol, identification and training requirements and assign appropriate internal staff	- Lack of cultural awareness - Competencies and skills not identified - No formal training program - Little or no in-house expertise or experience - General workforce unaware of risk management needs and lack training to adequately take ownership and control risks	- Competence, skills and training needs identified to achieve objectives and targets - Conducts training with some measure of competence to achieve objectives and targets - Focuses on addressing the identified issue(s) in the scope - Emphasizes awareness within the scope of the project	- Determines competence requirements that are necessary for activities defined in programs - Develops and implements an awareness program	- Identifies competencies and training needs associated with achieving the resilience objectives, targets and programs - Develops and implements a program to address competence and training needs - Assesses competence against requirements and ensure they are met	- Ensures that any person(s) performing tasks who have the potential to prevent, cause, respond to, mitigate, or be affected by significant hazards, threats, and risks are competent (on the basis of appropriate education, training, or experience - Retains associated training and competence records - Builds, promotes, and embeds a resilience management culture within the organization	- Builds, promotes, and embeds a resilience management culture within the organization, enterprise, supply chain and community - Ensures that the resilience management culture becomes part of the organization's core values and organization governance - Stakeholders are aware of the organizational resilience management policy and their role in any plans

Maturity Model for the Phased Implementation of the ANSI/ASIS.SPC.1:2009 Organizational Resilience Standard

ANSI/ASIS.SPC1 Standard Clause	Core Element	Issues Addressed by Core Element	Ad Hoc Approach Phase One	Project Approach Phase Two	Program Approach Phase Three	Systems Approach Phase Four	Management System Phase Five	Holistic Management Phase Six
		or support representatives. - Develops tools to enhance situational awareness.						
4.4.3 Communication and Warning	Communication and warning strategies, plans, programs and procedures	- Establishes procedures and makes arrangements for communication both within the organization and to/from external sources. - Documents procedures and identifies tools to manage relationships and communications processes with external stakeholders including supply chain business partners, first responders, governmental agencies, vendors, etc. - Develops, coordinates, evaluates and exercises plans to communicate information and warnings with internal stakeholders, external stakeholders (including the media) for normal and abnormal conditions. - Develops and maintains reliable communications and a warning capability in the event of a disruption.	- No formal procedures - Not coordinated internally or externally - Reactive in nature within predefined guidelines - Driven by demands for information	- Communication procedures address project objectives, target and scope - Develops communication procedures for internal and external stakeholders (including authorities and media) consistent with the project scope	- Identifies what will be communicated and to whom - Determines communications and warning needs - Establishes, implements, and maintains procedures for internal and external communications and warnings - Establishes calling trees and contact lists with authorities and roles in which to use them	- Identifies what will be communicated and to whom regarding the resilience policy, risks, objectives, targets and programs - Establishes communications feedback mechanisms - Identifies target audiences for communications and warnings to ensure effective two-way dialogue - Determines information sharing and security needs - Ensures ongoing communications capacity in the event of a disruptive incident	- Decides how proactive each type of communication should be with each audience - Develops key messages and set communication targets, objectives and performance indicators - Assigns responsibilities and establish timelines for communications - Establishes, documents and maintains procedures for internal and external communications - Communication on resilience issues occurs throughout the organization and with appropriate stakeholders - Structures communication with emergency and first responders - Determines needs and establish a communication facility - Sets communications protocols for normal and abnormal conditions - Regularly tests communications system	- Identifies external communications and warning needs and capacity of stakeholders supply chain and community - Determines reliability of external communications infrastructure and to augment system internally and externally in the event of a disruption
4.4.4 Documentation	Organizational resilience documentation	- Establishes processes and procedures for management of documents which are essential to the successful implementation and operation of the resilience management system and programs. - Documents the	- Informal if any	- Develops documented procedures to support action plans - Maintains documentation to support project scope - Documentation supports elements	- Develops a documents management program - Documentation supports elements address in program action plans	- Establishes resilience management documentation system - Determines security, sensitivity and information integrity needs and take appropriate steps to protect	- Develops and organizes documentation system - Prepares a resilience manual outlining the structure of the ORMS - Documentation supports the establishment, definition and implementation of the ORMS	- Evaluates document and information sharing needs with stakeholders, supply chain and community

Maturity Model for the Phased Implementation of the ANSI/ASIS.SPC.1:2009 Organizational Resilience Standard

ANSI/ASIS.SPC1 Standard Clause	Core Element	Issues Addressed by Core Element	Ad Hoc Approach Phase One	Project Approach Phase Two	Program Approach Phase Three	Systems Approach Phase Four	Management System Phase Five	Holistic Management Phase Six
		procedures, processes, work plans and forms to support the management system and its elements, as well as for use before, during and after a disruptive incident.		addressed in project		information and documentation		
4.4.5 Control of Documents	Documentation control	- Establishes processes and procedures for control of documents and records (including back-up) to protect the integrity and access to documentation and essential information.	- No document control system other than that used in general organizational operations	- Documents control using existing system with some procedures developed to help demonstrate success and business benefit - Rudimentary back-up of critical information	- Establishes processes and procedures for control of documents and records	- Establishes processes and procedures for control of documents and records for access, back-up confidentiality, storage, retention, archiving and destruction	- Establishes processes and procedures for control of documents and records including information security and protection and document integrity	- Evaluates stakeholder and supply chain information needs
4.4.6 Operational Control	Developing and implementing operational and risk control strategies, plans, procedures and programs	- Establishes operational control measures needed to implement the strategic plans and maintain control of activities and functions against defined targets, as well as the unexpected. - Develops procedures for controlling key activities, functions and operations that are associated with the organization. - Establishes processes and procedures for operational management and maintenance of infrastructure, plant, facilities, technologies, finance, etc. which have an impact on the organization's performance, its supply chain and stakeholders. - Establishes operational control measures needed to implement the	- Procedures and processes are undefined - Some individuals may address perceived potential problems on an ad-hoc basis	- Gives proper attention to operational controls and procedures to assure they will be performed properly to achieve objectives and target of issue(s) addressed within the scope	- Plans ways in which operations related to the organizations critical operations can be controlled based on outcomes of risk analysis or business impact analysis	- Identifies where controls are needed and what they will achieve in terms of risk reduction based on the risk assessment, objectives, targets and programs - Considers ways of minimizing risk in day-to-day operations - Priority is given to proactive approaches - Controls specify how to conduct activities and functions including engineering controls, administrative controls, technical specifications and contractual agreements	- Establishes, implements, and maintains adaptive and proactive procedures for those operations that are associated with the identified significant risks, consistent with its organizational resilience management policy, risk assessment, supply chain requirements, objectives, and targets, in order to ensure that they are carried out under specified conditions minimizing the risk - Control procedures are written and/or reviewed by persons involved in operations and communicated effectively to others such as contractors and suppliers	- Addresses reliability and resiliency, the safety and health of people, and the protection of property, supply chain and other stakeholder needs, and the environment potentially impacted by a disruptive incident - Ensures demand signals are comprehended in capacity planning - Priority is given to adaptive approaches - Ensures processes are in place to validate supplier responses

Maturity Model for the Phased Implementation of the ANSI/ASIS.SPC.1:2009 Organizational Resilience Standard

ANSI/ASIS.SPC1 Standard Clause	Core Element	Issues Addressed by Core Element	Ad Hoc Approach Phase One	Project Approach Phase Two	Program Approach Phase Three	Systems Approach Phase Four	Management System Phase Five	Holistic Management Phase Six
		strategic programs and maintain control of activities and functions. - Establishes and implements risk avoidance, mitigation, reduction, sharing and treatment procedures to minimize the likelihood and consequences of a disruptive incident.						
4.4.7 Incident Prevention, Preparedness, and Response	- Risk avoidance, mitigation, reduction, sharing and treatment procedures - Reactive, proactive, and adaptive incident management	- Establishes and implements risk avoidance, mitigation, reduction, sharing and treatment procedures to minimize the likelihood and consequences of a disruptive incident. - Establishes, documents and implements procedures and a management structure to prevent, prepare for, mitigate, and respond to a disruptive event using personnel. - Establishes, implements, and maintains procedures to avoid, prevent, protect from and mitigate a disruptive event. - Develops action plans for increased threat levels. - Establishes, implements, and maintains procedures to manage a disruptive event and continue its activities based on recovery objectives. - Establishes and documents procedures for how the organization will manage a disruptive event; and recover or maintain its activities to	- Little or no defined procedures - Dependence on the reactive behavior of individuals in the organization (and hope for the best)	- Defines procedures to assure they will be performed properly to achieve objectives and target of issue(s) addressed within the scope - Develops procedures to support action plans (including measures to reduce likelihood and/or consequences - Develops procedures based on identified issue(s) – may be predominately reactive in nature given that no formal risk assessment was conducted	- Identifies what emergency situations may occur and their potential impacts on critical assets, activities, services and functions - Develops procedures that prevent if possible, respond to and recover from potential disruptive events - Implements and tests the procedures - Considers measures that minimize both likelihood and consequences of a disruption but typically emphasis is on addressing consequences	- Based on the risk assessment, objectives, targets and programs, establishes, implements, and maintains procedures to identify potential disruptive incidents that can have impacts on the organization, its activities, functions, services, stakeholders, and the environment - Proactively documents with detailed procedures and work plans how the organization will prevent, prepare for, and respond to disruptive incidents - Periodically reviews and, where necessary, revises its incident prevention, preparedness, and response procedures	- Establishes, implements, and maintains procedures to avoid, prevent, protect from mitigate, respond to and recover from a disruptive event and continue its activities based on resilience objectives developed through the risk assessment process - Prepares for and responds to actual disruptive incidents to prevent the incident, minimize likelihood of its occurrence, or mitigate associated adverse consequences - Ensures that any persons performing incident prevention and management measures on its behalf are competent - Establishes, documents and implements procedures and a management structure to prevent, prepare for, mitigate, and respond to a disruptive event - Establishes detailed procedures for how the organization will respond to and manage a disruptive event and	- Identifies the organizations potential role in supporting the capacity of stakeholders, the supply chain and the community to avoid, prevent, protect from mitigate, respond to and recover from a disruptive event - Establishes detailed procedures for stakeholders, the supply chain and the community support

Maturity Model for the Phased Implementation of the ANSI/ASIS.SPC.1:2009 Organizational Resilience Standard

ANSI/ASIS.SPC1 Standard Clause	Core Element	Issues Addressed by Core Element	Ad Hoc Approach Phase One	Project Approach Phase Two	Program Approach Phase Three	Systems Approach Phase Four	Management System Phase Five	Holistic Management Phase Six
		a predetermined level.					how it will recover or maintain its activities to a predetermined level, based on management-approved recovery objectives	
4.5.1 Monitoring and Measurement	Performance evaluation	- Establishes metrics and mechanisms by which the organization assesses its ability to achieve its objectives and targets on an ongoing basis. - Monitors, measures, and assesses the organization's resilience performance on an ongoing basis.	- No formal monitoring - No formal measurement	- Progress against specific indicators are assess periodically with persons involved in relevant activities - Project indicators and metrics are established and monitored to demonstrate progress and performance improvement relative to identified issue(s)	- Identifies key characteristics that need monitoring and measuring - Plans what will be measured, where and when it will be measured and what methods will be used	- Establishes, implements, and maintains performance metrics and procedures to monitor and measure, on a regular basis, those characteristics of its operations that have material impact on its resilience performance	- Monitors performance, applicable operational controls, and conformity with the organization's organizational resilience management objectives and targets - Evaluates and documents the performance of the systems which protect assets, communications and information systems	- Includes partnership and supply chain relationships
4.5.2.1 Evaluation of Compliance	Compliance evaluation	- Monitors, measures, and assesses the organization's legal and regulatory compliance performance on an ongoing basis.	- No formal procedures established beyond those already in place as part of normal business operations	- Compliance evaluated related to issue(s) identified and the project scope	- Identifies and plans methods used to monitor and measure compliance	- Establishes, implements, and maintains procedure(s) for periodically evaluating compliance with applicable legal and other requirements	- Records and reports the results of the evaluation with corrective measures and recommendations for improvement	- Reports to relevant stakeholders as appropriate
4.5.2.2 Exercises and Testing	Testing and system evaluation	- Tests and evaluates appropriateness and efficacy of its ORMS, its programs, processes, and procedures (including stakeholder relationships and infrastructure interdependencies.) - Plans, coordinates, and conducts tests and exercises, and evaluates and documents results. - Reviews exercise results with management to ensure	- No exercising and testing	- Develops procedures for exercises and testing related to the identified project issue(s) - Results of exercises and texting are prepared in a report to demonstrate project performance and benefit in terms of enhanced	- Exercises and tests designed to evaluate the efficacy and implementation of action plans and procedures	- Validates the ORMS using testing and exercises - Tests and evaluates appropriateness and effectiveness of action plans and procedures as well as interrelationship of elements in ORMS - Includes appropriate external parties	- Tests and evaluates the appropriateness and efficacy of ORMS, its programs, processes, and procedures (including stakeholder relationships and infrastructure interdependencies) - Produces a formalized post-exercise report that contains outcomes, recommendations, and arrangements to implement improvements in a	- Tests and evaluates the appropriateness and efficacy of ORMS with stakeholders, supply chain and community

Maturity Model for the Phased Implementation of the ANSI/ASIS.SPC.1:2009 Organizational Resilience Standard

ANSI/ASIS.SPC1 Standard Clause	Core Element	Issues Addressed by Core Element	Ad Hoc Approach Phase One	Project Approach Phase Two	Program Approach Phase Three	Systems Approach Phase Four	Management System Phase Five	Holistic Management Phase Six
		lessons learned and appropriate action is taken.		resilience performance and business benefits		(e.g. first responders) and stakeholders	timely fashion	
4.5.3 Nonconformity, Corrective Action, and Preventive Action	<ul style="list-style-type: none"> - Analyzes and handles nonconformities - Improvement 	<ul style="list-style-type: none"> - Determines nonconformities and the manner in which these are dealt with. - Establishes and implements mechanisms for eliminating the causes of detected nonconformities both in the management system and the operational processes. - Establishes and implements mechanisms for instigating action to eliminate potential causes of nonconformities in both the management system and the operational processes. 	- Not defined	<ul style="list-style-type: none"> - Identifies deviations from action plans - Deviations from action plans, programs, objectives and targets are evaluated for opportunities for improvement - Adequate corrective and preventative actions taken if necessary to ensure the project progresses according to plan 	<ul style="list-style-type: none"> - Identifies deviations from action plans - Establishes a corrective action process - Identifies what went wrong and corrects it 	<ul style="list-style-type: none"> - Determines nonconformities in the ORMS, risk assessment, objectives, targets programs, action plans, and their implementation - Analyzes why something went wrong - Determines the manner in which they are dealt with to eliminate the causes and prevent their recurrence - Identifies what could go wrong and take actions to prevent occurrence 	<ul style="list-style-type: none"> - Establishes, implements, and maintains procedures for dealing with actual and potential nonconformities and for taking corrective action and preventive action - Reviews effectiveness of corrective actions and take preventative actions 	
4.5.4 Control of Records	Control of records	<ul style="list-style-type: none"> - Establishes and maintains records to demonstrate conformity to the requirements of its ORMS and the results achieved. 	- Not defined	<ul style="list-style-type: none"> - Collects and retains evidence addressing project implementation and results 	<ul style="list-style-type: none"> - Collects and retains evidence addressing program implementation and results 	<ul style="list-style-type: none"> - Collects and retains evidence addressing ORMS implementation and results 	<ul style="list-style-type: none"> - Collects and retains evidence addressing ORMS implementation and results 	
4.5.5 Internal Audits	System audits	<ul style="list-style-type: none"> - Conducts internal audits of system and programs. - Reports audits and verification results in management review. 	- Not conducted	<ul style="list-style-type: none"> - Performance of project audited informally - Project Leader oversees development of audit procedures 	<ul style="list-style-type: none"> - Conducts audit of program within defined scope and including all elements of the program 	<ul style="list-style-type: none"> - Determines what needs to be audited - Plans and implements an audit program - Reports audit findings to management and acts upon them 	<ul style="list-style-type: none"> - Responsibility of audit program assigned to an individual that has knowledge and understanding of audit principles - Determines whether the control objectives, risk controls, processes, and procedures of ORMS are conducted properly and achieving the desired results - Identifies opportunities for improvement - Ensures that actions are taken without undue delay to eliminate detected nonconformities and 	<ul style="list-style-type: none"> - Audit includes stakeholder and community interactions, as well the supply chain

Maturity Model for the Phased Implementation of the ANSI/ASIS.SPC.1:2009 Organizational Resilience Standard

ANSI/ASIS.SPC1 Standard Clause	Core Element	Issues Addressed by Core Element	Ad Hoc Approach Phase One	Project Approach Phase Two	Program Approach Phase Three	Systems Approach Phase Four	Management System Phase Five	Holistic Management Phase Six
							their causes	
4.6 Management Review	Management review	<ul style="list-style-type: none"> - Management review of the system determines its current performance, to ensure its continuing suitability, adequacy and effectiveness, and to instruct improvements and new directions when found necessary. - Sets priorities, policy, objectives and targets to support continual improvement. 	- No formal management review outside of existing fiscal reviews	- Project Leader supervisor (and other appropriate members of the management team) formally reports and reviews the performance of project	<ul style="list-style-type: none"> - Uses review to demonstrate business case for resilience management and provide a basis to seek further efficiencies by linking core elements in a systems approach - Management reviews the policies, objectives, evaluation of program implementation, audit results and changes resulting from preventive and corrective actions 	<ul style="list-style-type: none"> - Identifies inputs to review process - Reviews the suitability, adequacy and effectiveness of the ORMS 	<ul style="list-style-type: none"> - Top management reviews the ORMS at planned intervals to ensure its continuing suitability, adequacy, and effectiveness - Assesses opportunities for improvement and the need for changes to ORMS, including the organizational resilience management system policy and objectives, target and risk criteria 	<ul style="list-style-type: none"> - Integrates review with overall risk management and business review processes - Review includes evaluation of suitability, adequacy, and effectiveness with regard to stakeholders, community and supply chain
4.6.4 Maintenance	System maintenance	- Makes provisions for improvement of programs, systems, and/or operational processes.	- Not defined	- Project outcomes that improve resilience performance become standard operating procedures	- Program and action plans outcomes that improve resilience performance become standard operating procedures	- Ensures that any internal or external changes that impact the organization are reviewed in relation to the ORMS	- Identifies any new critical activities that need to be included in the ORMS program	- Ensures that any internal or external changes that impact the organization, the overall enterprise, stakeholders and the supply chain are reviewed in relation to the ORMS
4.6.5 Continual Improvement	Continual improvement	- Provisions made for continual improvement of the management system and resilience performance.	- Not defined	<ul style="list-style-type: none"> - Evaluation of project(s) - Evaluation of extension of scope to identify additional issues and expand project to management system 	<ul style="list-style-type: none"> - Evaluation of program - Evaluation of extension of scope to identify additional issues and expand program to management system 	- Continually improves the effectiveness of ORMS through the use of the organizational resilience management policy, objectives, audit results, analysis of monitored events, corrective and preventive actions, and management review	- Continually improves the effectiveness of ORMS through the use of the organizational resilience management policy, objectives, audit results, analysis of monitored events, corrective and preventive actions, and management review	- Continually improves the effectiveness of ORMS through the use of the organizational resilience management policy, objectives, audit results, analysis of monitored events, corrective and preventive actions, and management review