



ANSI/ASIS.SPC.1:2009 ORGANIZATIONAL RESILIENCE: SECURITY, PREPAREDNESS, AND CONTINUITY MANAGEMENT SYSTEMS – REQUIREMENTS WITH GUIDANCE FOR USE

INTERNAL AUDIT AND SELF ASSESSMENT FORM

Criteria	Evidence	Documents	Findings (Conformance or Opportunity for Improvement)				Conclusions	Comments
			Non = 0	Partial = 1	Full = 2	Opportunity For Improvement		
4.1.1 Define Scope of ORMS								
Scope of the ORMS defined and documented appropriate to the size, nature, and complexity of the organization								
Internal and external context and obligations (including legal responsibilities) considered in setting scope								
Consider critical operational objectives, assets, functions, services, and products								
Potential internal and external events, as well as unforeseen events and their potential impact that could adversely affect the critical operations and functions of the organization considered in setting scope								
Strategic weighting of likelihood and/or consequence reduction strategies defined based on the risk assessment and impact analysis								
4.2.1 Policy								
Top management defined, documented and provided resources for the organization's ORMS policy appropriate to the nature and scale of potential risks								

ANSI/ASIS SPC.1-2009, Organizational Resilience Standard - Internal Audit and Self Assessment Form - ASIS International

Includes a commitment to continual improvement and risk prevention, reduction and mitigation								
Includes a commitment to comply with applicable legal requirements and with other requirements to which the organization subscribes								
Provides framework for setting and reviewing ORMS objectives and targets								
Communicated to all persons working for or on behalf of the organization								
Reviewed at planned intervals and when significant changes occur								
Documented, implemented and maintained								
4.2.2 Management Commitment								
Management provided evidence of its commitment to establishment, implementation, operation, monitoring, review, maintenance and improvement								
Establish policy, targets and objectives								
Establish roles, responsibilities and competencies								
Appointed person(s) responsible for the ORMS								
Communicate to organization importance of ORMS								
Provide sufficient resources to establish, implement, operate, monitor, review, maintain and improve ORMS								
Set the criteria for accepting risks and the acceptable levels of risk								
Management participation in ORMS								
4.3.1 Risk Assessment and Impact Analysis								
Formal and documented process for risk assessment & impact analysis established, implemented, and maintained								
Asset identification and valuation conducted to identify organization's critical activities, functions, services, products, partnerships, supply chains, stakeholder relationships, and potential impact of disruptions								
Risk identification (threat assessment, vulnerability assessment, criticality assessment) conducted considering intentional, unintentional and naturally-caused disruptions								
Systematic risk analysis conducted								
Systematic risk evaluation conducted								
Recovery time objectives and priorities determined								
Cost-benefit analysis for risk treatments conducted								

ANSI/ASIS SPC.1-2009, Organizational Resilience Standard - Internal Audit and Self Assessment Form - ASIS International

Risk assessment taken into account in establishing, implementing, and operating ORMS								
Risk assessment re-evaluated with changing context								
Risk assessment inputs and outputs documented and kept up-to-date and confidential								
4.3.2 Legal and Other Requirements								
Procedures established and maintained to identify legal, regulatory, and other requirements to which the organization subscribes related to the organization's risks, assets, activities, functions, products, services, supply chain, the environment, and stakeholders								
Procedures established and maintained to determine how these requirements apply to the organization								
Information documented and kept it up-to-date								
Applicable legal, regulatory, and other requirements to which organization subscribes considered in ORMS								
4.3.3 Objectives, Targets and Programs								
Documented objectives and targets established and maintained to avoid, prevent, protect from, mitigate, respond to, and recover from disruptive incidents								
Programs based on risk assessment and impact analysis; and consistent with ORMS policy								
Establish expectations for other organizational relationships outside the boundary of the organization (such as suppliers) that are critical to mission accomplishment and functional operations								
Objectives and targets are measurable								
Risk treatment options selected based on legal, regulatory, and other requirements; risk assessment; technological options; its financial, operational, and business requirements; mutual aid agreements; and the views of stakeholders and other interested parties								
Programs include designation of responsibility and resources for achieving objectives and targets at relevant functions and levels of the organization								
Programs designate a means and time-frame								
Establish and maintain program for prevention and deterrence - Avoid, eliminate, deter, or prevent the likelihood of								

ANSI/ASIS SPC.1-2009, Organizational Resilience Standard - Internal Audit and Self Assessment Form - ASIS International

a disruptive incident and its consequences								
Establish and maintain program for mitigation - minimize the impact of a disruptive incident								
Establish and maintain program for emergency response - initial response to a disruptive incident involving protection of people and property from immediate harm								
Establish and maintain program for continuity - processes, controls, and resources are made available to ensure that the organization continues to meet its critical operational objectives								
Establish and maintain program for recovery - processes, resources, and capabilities of organization are re-established to meet ongoing operational requirements within time period specified in objectives								
4.4.1 Resources, Roles, Responsibility and Authority								
Management ensures availability of resources essential for implementation and control of ORMS								
Roles, responsibilities, and authorities defined, documented, and communicated for effective ORM								
Top management appointed specific ORMS management representative(s)								
ORM team established with appropriate authority to oversee incident prevention and management								
Logistical capabilities and procedures established to locate, acquire, store, distribute, maintain, test, and account for services, personnel, resources, materials, and facilities produced or donated to support ORMS								
Resource management objectives established for response times, personnel, equipment, training, facilities, funding, insurance, liability control, expert knowledge, materials, interdependencies, and time frames within which they will be needed								
Procedures established for stakeholder assistance, communications, strategic alliances, and mutual aid								
Financial and administrative procedures established to support the ORM program before, during, and after an incident								
4.4.2 Competence, Training and Awareness								
Ensured that any persons performing tasks who have the potential to prevent, cause, respond to, mitigate, or be affected by								

ANSI/ASIS SPC.1-2009, Organizational Resilience Standard - Internal Audit and Self Assessment Form - ASIS International

significant risks are competent (based on appropriate education, training, or experience)								
Identify training competencies and needs associated with incident prevention and management; and ORMS								
Provide training or take other action to meet competency needs and retain associated records								
Establish, implement, and maintain procedures to ensure persons working for it or on its behalf are aware of: a) The significant hazards, threats, and risks, and related actual or potential impacts, associated with their work and the benefits of improved personal performance; b) The procedures for incident prevention, deterrence, mitigation, self-protection, evacuation, response, continuity, and recovery; c) The importance of conformity with the ORM policy and procedures and with the requirements of the ORMS; d) Their roles and responsibilities in achieving conformity with the requirements of the ORMS; e) The potential consequences of departure from specified procedures; and f) The benefits of improved personal performance.								
Build, promote, and embed an ORM culture that: a) Ensures the ORM culture becomes part of the organization's core values and organization governance; and b) Makes stakeholders aware of the ORM policy and their role in any plans.								
4.4.3 Communication and Warning								
Procedures established, implemented and maintained for internal communication and consultation between the various levels and functions of the organization								
Procedures established, implemented and maintained for external communication and consultation with partner entities and other stakeholders								
Procedures established, implemented and maintained for receiving, documenting, and responding to communication from external stakeholders								
Procedures established, implemented and maintained for adapting and integrating a national or regional risk or threat advisory system into planning and operations								
Procedures established, implemented and maintained for alerting stakeholders potentially impacted by an actual or impending disruptive incident								
Procedures established, implemented and maintained for assuring availability of the means of communication during a crisis								

ANSI/ASIS SPC.1-2009, Organizational Resilience Standard - Internal Audit and Self Assessment Form - ASIS International

situation and disruption								
Procedures established, implemented and maintained for facilitating structured communication with emergency responders								
Procedures established, implemented and maintained assuring the interoperability of multiple responding organizations and personnel								
Procedures established, implemented and maintained for recording of vital information about the incident, actions taken, and decisions made								
Procedures established, implemented and maintained for operations of a communications facility								
Procedures established, implemented and maintained for external communication, alerts, and warnings (including with the media)								
Communications systems tested regularly								
4.4.4 Documentation								
Documentation includes: a) The ORM policy, objectives, and targets; b) Description of the scope of the ORMS; c) Description of the main elements of the ORMS and their integration with related documents; d) Documents, including records, required by the Standard; e) Documents, including records, determined by organization to be necessary to ensure effective planning, operation, and control of processes that relate to its significant risks.								
4.4.5 Control of Documentation								
Establish, implement, and maintain (a) procedure(s) to: a) Approve documents for adequacy prior to issue; b) Review, update and re-approve documents as necessary; c) Ensure that changes and current revision status of documents are identified; d) Ensure that relevant versions of applicable documents are available at points of use; e) Establish document retention and archival parameters; f) Ensure that original and archival copies of documents, data, and information remain legible and readily identifiable; g) Ensure that documents of external origin determined by the organization to be necessary for the planning and operation of the ORMS are identified and their distribution controlled; h) Identify as obsolete all out-of-date documents that the organization is required to retain; and i) Ensure the integrity of the documents by ensuring they are tamperproof, securely backed-up, accessible only to authorized personnel, and protected from damage, deterioration, or loss.								

4.4.6 Operational Control							
Operating criteria stipulated by establishing, implementing, and maintaining documented procedures to minimizing the likelihood and/or consequences of a disruptive incident related to the organization's internal and external activities							
Adaptive and proactive procedures established, implemented, documented and maintained for operations related to the identified risks to the activities, functions, products, and services of the organization and communicating applicable procedures and requirements to suppliers (including contractors)							
Procedures established, implemented and maintained related to control potential incidents consistent with ORM policy, risk assessment, objectives, and targets							
Establish, implement and maintain procedures to address reliability and resiliency, safety and health of people, and protection of property and the environment impacted by a disruptive incident							
4.4.7 Incident Prevention, Preparedness, and Response							
Procedures established, implemented, and maintained to prevent and manage disruptive events that have the potential to harm the organization and its supply chain partners based on risk assessment							
Procedures established, implemented, documented and maintained to: a) avoid, remove or reduce the likelihood of a disruptive event; b) reduce the consequences of a disruptive event; c) protect people, physical assets and critical information including records from immediate harm; d) maintain continuity of essential services; e) recover from a disruptive event.							
Develop and implement incident prevention and management procedures to minimize the likelihood of a disruptive event or to minimize the potential for the severity of the consequences of the event. a) Prevention procedures should describe how the organization will take proactive steps to protect its assets by establishing architectural, administrative, design, operational and technological approaches to avoid, eliminate or reduce the likelihood of risks materializing, including the protection of assets from unforeseen threats and hazards. b) Mitigation procedures should describe how the organization will take proactive steps to protect its assets by establishing immediate, interim and long-term approaches to reduce the consequences of risks before they materialize,							

ANSI/ASIS SPC.1-2009, Organizational Resilience Standard - Internal Audit and Self Assessment Form - ASIS International

including the protection of assets from unforeseen threats and hazards.								
Develop and implement response plans that describe how the organization will respond to one or more types of disruptive event.								
Develop and implement continuity plans that describe how the organization will maintain and/or re-establish critical activities in the period immediately following the response/emergency phase.								
Develop and implement incident prevention and management procedures with regard to: a) The nature of onsite hazards (e.g., flammable and toxic materials, storage tanks, compressed gases) and measures to be taken in the event of a disruptive incident or accidental releases; b) The nature of local, nearby, or other external hazards with a potential impact on the organization; c) The most likely type and scale of a disruptive incident; d) Procedures to prevent environmental damage.								
Develop and implement incident response and management procedures with regard to: a) The most appropriate method(s) for mitigation and emergency response to a disruptive incident to avoid escalation to a crisis or disaster; b) Command and control procedures for and structure of pre-defined chain of command, (an) emergency operations center(s), and/or (an) alternate worksite(s); c) Procedures and authority to declare an emergency situation, initiate emergency procedures, activate plans and actions, assess damage, and make financial decisions; d) Internal and external communication plans including notification of appropriate authorities and stakeholders; e) Procedures to acquire and/or provide appropriate medical care; f) The action(s) required to minimize human casualties, and physical and environmental damage; g) The action(s) required to secure vital information, information systems, facilities, and people; h) Mitigation and response action(s) to be taken for different types of disruptive incident(s) or emergency situation(s); i) The need for (a) process(es) for post-event evaluation to establish and implement corrective and preventive actions; j) Periodic testing of incident and emergency management and response procedure(s) and processes;								
Develop and implement incident management procedures addressing: a) Training of incident and emergency response personnel; b) A list of key personnel and aid agencies,								



ANSI/ASIS SPC.1-2009, Organizational Resilience Standard - Internal Audit and Self Assessment Form - ASIS International

including contact details (e.g., first responders, law enforcement, hazmat clean-up services); c) Evacuation routes and assembly points including lists of personnel and contact details; d) The potential for (a) disruptive incident or emergency situation(s) to affect or be affected by critical infrastructure (e.g., electricity, water, communications, transportation); e) The possibility of mutual assistance to and from neighbouring organizations.								
Develop and implement recovery plans that describe how the organization will re-establish all necessary operational and support activities, replace damaged and/or destroyed assets and information, rebuild brand and reputation of the organization, and assist staff to recover from the event.								
Periodically review and, where necessary, revise its incident prevention and management procedures – in particular, after the occurrence of accidents or incidents that can escalate into an emergency, crisis, or disaster.								
Ensure that any person(s) performing incident prevention and management measures on its behalf are competent on the basis of appropriate education, training, or experience, and retain associated records.								
Document this information and updated it at a regular interval or as changes occur.								
4.5 Checking								
ORM plans, procedures, and capabilities evaluated through periodic assessments, testing, post-incident reports, lessons learned, performance evaluations, and exercises. Significant changes in these factors are reflected immediately in the procedures.								
Keep records of the results of the periodic evaluations.								
4.5.1 Monitoring and Measurement								
Performance metrics and procedures established, implemented, and maintained to monitor and measure, on a regular basis, those characteristics of its operations that have material impact on its performance (including partnership and supply chain relationships).								
Documented information to monitor performance, applicable operational controls, and conformity with the organization's ORM objectives and targets.								
Performance of procedures and systems which protect its assets, activities, communications and information systems, evaluated, documented and reviewed.								

4.5.2.1 Evaluation of Compliance							
Procedures for periodically evaluating compliance with applicable legal, regulatory and other requirements to which it subscribes established, implemented, and maintained							
Non-conformances in compliance are reviewed and address with corrective and preventive actions.							
Keep records of the results of the periodic evaluations							
4.5.2.2 Exercises and Testing							
Exercise and testing procedures established, implemented, documented and maintained to evaluate the appropriateness and efficacy of ORMS, its programs, processes, and procedures (including partnership and supply chain relationships).							
Validate the ORMS using exercises and testing that: <ul style="list-style-type: none"> a) Are consistent with the scope of the ORMS and objectives of the organization; b) Are based on realistic scenarios that are well planned with clearly defined aims and objectives; c) Minimize the risk of disruption to operations and the potential to cause risk to operations and assets; d) Produce a formalized post-exercise report that contains outcomes, recommendations, and arrangements to implement improvements in a timely fashion; e) Are reviewed within the context of promoting continual improvement; and f) Are conducted at planned intervals, and from time to time on a non-periodic basis as determined by the management of the organization, as well as when significant changes occur within the organization and the environment it operates in. 							
4.5.3 Nonconformity, Corrective Action, and Preventive Action							
Procedures established, implemented, and maintained for dealing with actual and potential nonconformities and for taking corrective action and preventive action.							
Procedures established that define requirements for: <ul style="list-style-type: none"> a) Identifying and correcting nonconformity(ies) and taking action(s) to mitigate their impacts; b) Investigating nonconformity(ies), determining their cause(s), and taking actions in order to avoid their recurrence; c) Evaluating the need for action(s) to prevent nonconformity(ies) and implementing appropriate actions designed to avoid their occurrence; d) Recording the results of corrective action(s) and preventive action(s) taken; and e) Reviewing the effectiveness of corrective action(s) and preventive action(s) taken. 							

ANSI/ASIS SPC.1-2009, Organizational Resilience Standard - Internal Audit and Self Assessment Form - ASIS International

Actions taken are appropriate to the impact of the potential problems, and conducted in an expedited fashion.								
Identify changed risks, and identify preventive action requirements focusing attention on significantly changed risks.								
Priority of preventive actions are determined based on the results of the risk assessment and impact analysis.								
Make any necessary changes to the ORMS documentation.								
4.5.4 Control of Records								
Establish and maintain records to demonstrate conformity to the requirements of its ORMS and of the Standard and the results achieved.								
Establish, implement, and maintain (a) procedure(s) to protect the integrity of records including access to, identification, storage, protection, retrieval, retention, and disposal of records.								
Records are legible, identifiable, and traceable.								
4.5.5 Internal Audits								
ORM audit program and procedures established, implemented and maintained ensure that internal audits of the ORMS are conducted at planned intervals.								
Audit procedures determine whether objectives, controls, processes, and procedures of its ORMS: a) Conform to the requirements of the Standard and relevant legislation or regulations; b) Conform to risk management requirements; c) Are effectively implemented and maintained; d) Perform as expected.								
Audit criteria, scope, frequency, and methods are defined.								
Selection of auditors and conduct of audits ensures objectivity and impartiality of the audit process.								
Responsibilities and requirements for planning and conducting audits, reporting results and maintaining records are defined in a documented procedure.								
Management ensures actions taken without delay to eliminate detected nonconformities and their causes.								
Follow-up activities include the verification of the actions taken and the reporting of verification results.								
4.6 Management Review								
Management reviews ORMS system at planned intervals to ensure its continuing suitability, adequacy, and effectiveness.								

ANSI/ASIS SPC.1-2009, Organizational Resilience Standard - Internal Audit and Self Assessment Form - ASIS International

Review includes assessing opportunities for improvement and the need for changes to ORMS, including the ORMS policy and objectives.								
Input to management review includes: a) Results of ORMS audits and reviews; b) Feedback from interested parties; c) Techniques, products, or procedures that could be used in the organization to improve the ORMS performance and effectiveness; d) Status of preventive and corrective actions; e) Results of exercises and testing; f) Vulnerabilities or threats not adequately addressed in the previous risk assessment; g) Results from effectiveness measurements; h) Follow-up actions from previous management reviews; i) Any changes that could affect the ORMS; j) Adequacy of policy and objectives; and k) Recommendations for improvement.								
Output from the management review includes any decisions and actions related to the following: a. Improvement of the effectiveness of the ORMS; b. Update of the risk assessment, impact analysis, and incident preparedness and response plans; c. Modification of procedures and controls that effect risks, as necessary, to respond to internal or external events that may impact on the ORMS, including changes to: i. Business and operational requirements; ii. Risk reduction and security requirements; iii. Operational conditions processes effecting the existing operational requirements; iv. Regulatory or legal requirements; v. Contractual obligations; vi. Levels of risk and/or criteria for accepting risks. d. Resource needs; and e. Improvement to how the effectiveness of controls is being measured.								
4.6.4 Maintenance								
Top management establishes a defined and documented ORMS maintenance program to ensure that any internal or external changes that impact the organization are reviewed in relation to the ORMS.								
Identify any new critical activities that need to be included in the ORMS maintenance program.								
4.6.5 Continual Improvement								
Continually improve the effectiveness of the ORMS through the use of the ORM policy, objectives, audit results, analysis of monitored events, corrective and preventive actions, and management review.								