ACCREDITATION RULE 52
Issue Date: 2018/07/09
Implementation Date: 2018/07/09
Supersedes: 2017/02/10

SUBJECT: Accreditation Program for ASIS SPC.1 Security, Preparedness, and Continuity Management Systems and PS-Prep™

APPLIES TO: ANAB-Accredited and Applicant Certification Bodies

PREFACE

This Accreditation Rule is to inform certification bodies (CBs) of ANAB requirements for accreditation to certify organizations for ASIS SPC.1 security and resilience management systems and the Voluntary Private Sector Preparedness (PS-Prep) Program. Requirements for other preparedness and PS-Prep standards are in Accreditation Rules 51 and 53.

ACCREDITATION RULE

1. Requirement Documents (current versions unless specified)
   1.2. ISO/IEC 17021-1, Conformity assessment – Requirements for bodies providing audit and certification of management systems
   1.3. ANSI/ASIS SPC.2, Annex A, Required knowledge and skills of resilience auditors
   1.4. MA 5000, ANAB Accreditation Manual, and applicable ANAB Accreditation Rules
   1.5. IAF Mandatory Documents as applicable

2. Application Process
   2.1. CBs can obtain applications for informational use at www.anab.org.
   2.2. The application process outlined at www.anab.org must be completed via ANAB’s Enterprise Quality Manager (EQM) database when the CB is ready to apply for accreditation.
   2.3. The application fee includes the cost of one assessor day for the off-site documentation review.

3. Initial Assessments for Accreditation
   3.1. An ANAB accreditation assessor shall conduct a full documentation review.
   3.2. After the documents are found acceptable, ANAB shall conduct an office assessment and required witnessed audits.
      3.2.1. The office assessment shall be conducted on site or remotely (at ANAB’s discretion) and is conducted to ensure the CB’s certification process for security and resilience management systems conforms with ISO/IEC 17021-1 and is effective.
      3.2.2. ANAB shall witness the CB conducting a two-stage audit process (stages 1 and 2).
         3.2.2.1. The ANAB assessment team shall have the same number of members as the CB audit team.
      3.2.3. If the CB applies for ASIS SPC.1 and any additional preparedness standards, ANAB will determine the witnessing required for initial accreditation based on factors including but
not limited to the CB’s clients and their scopes of certification; the application review, including the CB’s competence process for personnel for all preparedness standards for which the CB applies; and office assessment results, if available.

3.2.3.1. If one witnessed audit is used for accreditation for more than one preparedness standard, ANAB requires witnessing the first available two-stage audit process (stages 1 and 2) for the other standard(s), but no later than the end of the first accreditation cycle.

4. Surveillance Assessments

4.1. ANAB shall conduct an annual office assessment and annually witness a CB team conducting an ASIS SPC.1 audit.

4.1.1. When possible, the office assessment shall be conducted concurrently with assessments for other ANAB accreditation programs for which the CB is accredited.

4.1.2. During the accreditation cycle, ANAB shall evaluate the CB’s full system audit process during at least one annual witnessed audit (stages 1 and 2 certification audit or recertification). The additional witnessed audits required in the accreditation cycle are based on the CB’s audit activity and management system findings, and include audit types such as surveillance, special, multi-site, scope expansion, transfer, integrated, ASRP, and/or CAAT. ANAB Accreditation Rule 18 outlines the witnessed audit scheduling process and the process for potentially altering the types of audits witnessed.

4.1.3. If the CB is accredited for ASIS SPC.1 and any other preparedness standards, ANAB will structure the witnessing and assessment program, taking into consideration the CB’s activity for each standard, results of previous assessments, etc.; however, ANAB shall witness all preparedness standards at least once during the accreditation cycle.

5. Reaccreditation Assessments

5.1. ANAB shall conduct a document review and an on-site full system office assessment at approximately six months prior to the expiration of accreditation.

6. Competence of CB Personnel

6.1. The CB shall follow the requirements of Annex A of ANSI/ASIS SPC.2 and Annex 1 of this Accreditation Rule when determining the competence criteria for security and resilience.

6.2. The CB shall ensure that its auditors have successfully completed a training course that includes an examination to assess the knowledge required to audit to ASIS SPC.1.

7. End User Expected Outcomes for Accredited Certification to ASIS SPC.1

7.1. End users can expect an organization with a certified security and resilience management system to better anticipate, protect, prevent, respond to, and recover from undesirable and disruptive events. Certification of a management system for security, resilience, and/or business continuity can provide assurance that the organization is able to avoid and prevent undesirable and potentially disruptive events, protect its assets, quickly respond to mitigate negative impacts, and promptly recover to full operational capacity.

7.2. The CB shall have processes to ensure that its auditors and other certification personnel are knowledgeable of the expected outcomes and consistently reinforce them with the CB’s clients.

8. Additional Requirements for PS-Prep

8.1. The CB may become accredited to offer certification for PS-Prep for ASIS SPC.1, as a standard recognized by the U.S. Department of Homeland Security (DHS).

8.2. Upon PS-Prep accreditation, the CB shall execute a sub-license agreement with ANAB to use the DHS-owned PS-Prep mark in accordance with DHS style material provided by ANAB.
8.2.1. Upon certifying an organization for PS-Prep, the CB shall sub-license the certified organization to use the DHS-owned PS-Prep mark in accordance with the DHS style material.

8.3. The CB shall populate ANAB’s EQM database with required PS-Prep client information.
Annex 1. Competencies

This appendix specifies competence requirements in addition to those specified in ISO/IEC 17021-1 and the competence requirements specified in ANSI/ASIS SPC.2, Annex A. During its competency needs analysis, the CB is expected to consider each auditor individually and the competence required. The CB shall maintain records of the needs analysis for each auditor.

The following competencies are not an exhaustive listing for audit team members and the CB is expected to identify additional and appropriate competencies for all affected personnel during its competency needs analysis.

General

The CB’s audit team members shall have demonstrated the competence to:

- Evaluate the appropriate level of connectivity or relationship of the standard’s requirements to the organization’s culture.
- Evaluate the appropriate level of how the organization fits into an enterprise-wide system if part of a larger entity.
- Understand the purpose of documentation requirements and control of documents and whether they meet the requirements of the standard.
- Understand the sensitivity and proprietary nature of risk-related information.
- Understand the application of documents required by laws and regulations.
- Understand the application of laws and regulations for the organization’s industry sector.
- Evaluate the effectiveness of management’s commitment to the program.

Planning

The CB’s audit team members shall have demonstrated the competence to:

- Evaluate that the organization’s scope of the organizational resilience management system is adequate to ensure organizational resilience under all conditions.
- Evaluate that the organization’s policy statement reflects the requirements of the standard.
- Evaluate that an organization has an effective process for risk assessment and impact analysis to address intentional, unintentional, and naturally-caused hazards and threats that have the potential for a direct or indirect impact on the organization’s operations; function; human, intangible, and physical assets; the environment; and its stakeholders.
- Understand the impact of the organization’s policy, scope, and objectives on its operations and whether or not they have been taken into account during planning stages.
- Understand if the organization’s personnel competency requirements are appropriate to the policy, scope, objectives, and targets.

Implementation/Operation

The CB’s audit team members shall have demonstrated the competence to:

- Evaluate the organization’s risk assessment methodologies, including threat/opportunity analysis, vulnerability/capability analysis, and criticality/consequence analysis.
- Understand the organization’s dependencies and interdependencies, including supply chain risk for the industry sectors to be audited.
- Evaluate that an organization’s risk strategies to adaptively, proactively, and reactively address minimization of both the likelihood and consequences of undesirable and disruptive events are appropriate.
- Understand techniques used to develop and implement the system.
- Evaluate the level to which the organization has planned, organized, directed, and managed its system.
- Determine whether strategies are consistent with management policy, stated goals and objectives, and managing risks related to undesirable and disruptive events.
- Determine the availability and capability of resources to adequately manage identified or potential risks.
• Determine whether the roles, responsibilities, and authorities assigned to manage and implement the system are adequate to meet objectives.
• Understand plan requirements for incident prevention, preparedness, response, continuity, and recovery.
• Understand communication planning for assessing and managing risks.
• Understand the laws and regulations requiring prevention and risk mitigation programs.
• Understand the prevention and risk mitigation strategies and methodologies for the industry sectors to be audited.
• Determine whether the training and awareness programs are appropriate for the risks identified in the risk assessment.
• Determine whether the system includes implemented strategies to manage risks related to undesirable and disruptive events commensurate with the frequency of identified hazards and the potential severity of impacts.

**Monitoring and Evaluation**

The CB’s audit team members shall have demonstrated the competence to:
• Understand exercise and testing methodologies commensurate with the risks identified in the risk assessment.
• Review testing and exercise records to determine whether the monitoring program has achieved program goals and objectives and required capabilities have been established.
• Comprehend whether or not the monitoring, measurement, internal audit, and evaluation activities are appropriate for the organization and the industry sector in which it operates.

**Review**

The CB’s audit team members shall have demonstrated the competence to:
• Comprehend whether the review, preventive and corrective action, and continual improvement activities are commensurate with the organization’s goals and objectives.
• Comprehend whether the management review activities are commensurate with the geographical location and industry sector in which the organization operates and the input and output requirements of the standard.