



ACCREDITATION RULE 24
Issue Date: 2011/03/24
Implementation Date: 2011/03/24
Supersedes: 2008/04/22

SUBJECT: Accreditation Program for Supply Chain Security Management Systems (SCSMS)

APPLIES TO: ISO 28000 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 SCSMS conforming with ISO 28000, Specification for security management systems for the supply chain.

ACCREDITATION RULE

1. Requirement Documents (current versions)
 - 1.1. ISO 28003, Security management systems for the supply chain – Requirements for bodies providing audit and certification of supply chain management systems
 - 1.2. ISO 28000, Specification for security management systems for the supply chain
 - 1.3. ISO/IEC 17021, Conformity assessment – Requirements for bodies providing audit and certification of management systems
 - 1.4. MA 6000, ANAB Accreditation Manual, and applicable ANAB Accreditation Rules
 - 1.5. IAF Mandatory Documents as applicable
2. Prerequisites
 - 2.1. A CB shall conform with ISO/IEC 17021.
3. Application Process
 - 3.1. SCSMS applicant CBs can obtain an application for informational use at www.anab.org.
 - 3.2. The application process outlined at <http://www.anab.org/certification-bodies/become-a-certification-body.aspx> must be completed via ANAB's Enterprise Quality Manager (EQM) database when the CB is ready to apply for SCSMS accreditation.
 - 3.3. The application fee includes the cost of one assessor day for the off-site documentation review.
4. Initial Assessment and Accreditation
 - 4.1. An ANAB accreditation assessor shall conduct a full documentation review.
 - 4.2. After the documents are found acceptable, ANAB shall conduct an on-site office assessment and witnessed audit.
 - 4.2.1. The office assessment shall be conducted to ensure the CB's certification process for SCSMS conforms with ISO/IEC 17021 and ISO 28003.
 - 4.2.2. ANAB shall witness the CB conducting a two-stage audit process (stages 1 and 2).
 - 4.2.2.1. The stage 2 SCSMS audit shall be conducted by a team of at least two auditors of the CB.

4.2.2.2. The ANAB assessment team shall have the same number of members as the CB audit team.

5. Ongoing Surveillance

5.1. ANAB shall conduct an annual office assessment and annually witness a CB team (a team may consist of one auditor) conducting an SCSMS audit.

5.1.1. The office assessment shall be conducted concurrently with other ANAB accreditation programs for which the CB is accredited.

5.1.2. Annual witnessed audits may be surveillance audits; however, one annual witnessed audit in the accreditation cycle shall evaluate the CB's recertification process and one annual witnessed audit in the accreditation cycle shall evaluate the CB's initial certification audit (stages 1 and 2) process.

6. Re-accreditation

6.1. The SCSMS accreditation period initially shall be four years *or* shall be established to coincide with the CB's current accreditation period (if any), and thereafter shall be four years.

6.2. ANAB shall conduct a document review and an on-site office assessment and witnessed audit.

6.2.1. The required witnessing of a CB's initial audit (stages 1 and 2) may be achieved any time within the accreditation cycle; however, it must be completed prior to re-accreditation.

7. Audit Duration

7.1. For each client, the CB shall document the justification for the audit duration and maintain records of the audit duration and justification.

8. Audit Team Competence

8.1. In addition to the demonstrated knowledge, skills, and attributes for competence of a management systems audit team, a CB shall demonstrate each audit team has the additional knowledge as follows:

8.1.1. Be able to judge conformance or nonconformance with ISO 28000.

8.1.2. Be able to make sound judgments when auditing an organization's processes for:

8.1.2.1. Change management.

8.1.2.2. Risk assessment and analysis.

8.1.2.3. Vulnerability assessment and threat identification.

8.1.2.4. Incident planning, preparedness, and response.

8.1.2.5. Handling confidential information.

8.1.2.6. Post-incident recovery and actions.

8.1.3. Be able to make sound judgments when auditing risk control, minimization, mitigation, and elimination methodologies.

8.1.4. Be able to understand and apply governmental and intergovernmental regulations, initiatives, and programs that have an impact on supply chain security.

8.1.5. Be able to make sound judgments when auditing an organization's supply chain process flow.