



ACCREDITATION RULE 36
Issue Date: 2010/05/17
Implementation Date: 2010/05/17
Supersedes: New

SUBJECT: Access by Auditors Being Denied on Security Grounds

APPLIES TO: ANAB Accredited Certification Bodies

PREFACE

This Accreditation Rule is to inform certification bodies (CBs) of ANAB requirements when being denied access by certified organizations or those seeking initial certification to facilities or systems in the course of undertaking management system audits.

ACCREDITATION RULE

Requirements Documents

- ISO/IEC 17021 Conformity assessment – Requirements for bodies providing audit and certification of management systems
- ANAB Accreditation Rule 9, Compliance with Legislation and Regulatory Requirements (related document)

Background

There are instances of auditors being denied access for various reasons when undertaking management system audits. Some organizations deny auditors access to proprietary or classified information, systems, and/or areas within a facility because of competitive sensitivity, national security regulations invoked in customer contracts, or other reasons.

CB Action

The CB and client shall develop an audit strategy for classified areas and/or limited access areas.

The CB shall require the organization to provide specific information at the contract development stage if any processes, activities, programs, specifications, systems, areas, or facilities are not made accessible because of security, confidentiality, or other restrictions. If such restrictions occur, the CB shall ensure that the scope of certification shall not include the processes, activities, programs, specifications, systems, areas, or facilities that will not be audited to sufficient depth to verify an organization's conformity to the related standard(s), including determination of effectiveness of the management system to the standard(s).

All information obtained at the contract stage shall be used, as appropriate, at the auditor assignment and audit planning stages.

If it is not possible to determine conformity without first undertaking an audit, then the audit must ensure that the processes can be proven to be similar to processes that were assessed in the unrestricted areas of the organization and that the same management system procedures and controls are applied and used within the restricted area. The audit report shall clearly and

unambiguously document all exclusions for these programs, customers, and/or activities, with supporting justification provided.

Given adequate time, a method that may be adopted is to have an area or document sanitized to the extent that an auditor can have access to validate conformance but still be sufficient enough not to compromise the integrity of the reports so that effective certification decisions can be made.

Another method is for the client and CB to mutually agree to identify and use “trusted contacts” (individuals or a specific department or group) to work with the CB auditor and the client organization to obtain the necessary evidence to validate conformance. These “trusted contacts” will be client resources with higher security clearances to enable a thorough review of classified documents that a CB’s auditors cannot review. The “trusted contact” resource shall demonstrate independence and impartiality to the greatest extent possible.

Some industry sector rules (e.g., AS9104/1) may document their own requirements for access and control of access to restricted areas, in which case the sector requirements will take precedence over this Accreditation Rule.