QCI – CAPSI Voluntary Initiative

Security sTar Agencies Rating Scheme

Requirements for Certification Bodies

TABLE OF CONTENTS

0. Introduction

0.1 **Quality Council of India (QCI)**, India's apex quality facilitation and national accreditation body, and the **Central Association of Private Security Industry (CAPSI)**, the preeminent organization for security professionals, have signed an MoU to operate a voluntary certification and rating programme for Private Security Agencies. This process of standardization will help the Agencies enhance their credibility and consequently their business.

While **QCI and CAPSI are the joint Scheme owners**, the governing structure of the initiative is under a multi stakeholder **Steering Committee** and the initiative would be operated on a non-profit but self-sustaining basis. It would have a defined **consensus based technical criteria** laid down for the Private Security Agencies who would be evaluated by competent third party certification bodies, To identify the competence of certification bodies' auditors for evaluation of technical criteria as devised and certification process, a multi stakeholders Certification committee has been formed. Certification bodies in turn would be accredited by the **National Accreditation Board for Certification Bodies (NABCB)**, which is part of the international system of equivalence of accreditations and certifications, as per appropriate international standards.

0.2 The Private Security Agency requiring certification under this **Security sTar Agencies Rating Scheme (STAR)** is required to be certified ultimately by an NABCB accredited Certification Body duly approved by the Quality Council of India, as the joint Scheme owner, and complying with the requirements as specified under this Scheme. The requirements that the Certification bodies need to comply with for getting approved by QCI under this Scheme are detailed in this document.

0.3 Initially, certification bodies would need provisional approval under the Scheme the system for which is described in the document Provisional Approval System for Certification Bodies separately.

1. Scope and Purpose

1.1 This document specifies the **"QCI – CAPSI Voluntary Certification and Rating Scheme for Private Security Agencies"** here in after known as **Security sTar Agencies Rating Scheme (STARS)**, specific additional requirements that the certification bodies need to fulfil in order to be accredited by NABCB for the STAR Scheme operated by the Quality Council of India.

1.2 The certification bodies approved under the STAR Scheme shall be able to offer the certification for the following levels;

Level 1 – One Star – **Meeting Compliance Requirements**

Level 2 – Two Star – **Established Compliance Management**

Level 3 – Three Star – **Consistent Operations**

Level 4 – Four Star – **Sustained Performance**

Level 5 – Five Star – **Assured Quality**

Level 6 – Six Star – **Trusted Excellence**

Level 7 – Seven Star – **Professionally Managed Security Operations**

1.3 In order to be able to offer certification for the Level 1 to 7, the certification bodies shall need to be accredited by as per ISO 17021-1:2015 NABCB as per the following requirements read with additional requirements specified in this document and shall have undergone a witness assessment by NABCB.

1.4 However if above criteria in 1.3 is not met then a certification body can be granted a provisional QCI approval for Private Security Agency Certification as per Provisional Approval System for Certification Bodies, for a period of one year subject to condition that certification bodies gets accredited by NABCB as per 1.3 above.

1.5 The requirements prescribed in this document are additional requirements that the certification body shall fulfil. Irrespective of which level under the scheme, the certification body opts for, the requirements mentioned in each clause shall apply.

1.6 If CB applies to NABCB to include STAR Schemes as extension of scope in their existing QMS accreditation, they may opt for either NABCB office assessment for scope extension assessment in which STAR Schemes would be reviewed and recommended for QCI provisional approval or they may opt for QCI assessment for STAR Schemes and latter for NABCB scope extension. NABCB would advise the CB about the options available

2. General Requirements

2.1 Legal and Contractual Matters

2.1.1 In addition to the requirements as specified in the accreditation standard (clause 5.1 of ISO 17021-1:2015) following requirements shall apply:

2.1.2 Certification agreement

2.1.2.1 The certification body shall ensure that its certification agreement requires that the client comply with the following requirements in addition to those specified in the respective standards as above:

a) Always fulfill the certification requirements as specified in the STARS Technical criteria document, the certification process described in the document “Security sTar Agencies Rating Scheme - Certification Process for Systems Certification”, the requirements specified in this document, as applicable, and the changes in them as communicated by the certification body from time to time;

b) The certified Private Security Agency and its processes always fulfils the certification requirements;

c) The liability on account of non-conforming processes/ services shall rest with the certified Private Security Agency.

d) The agency makes all necessary arrangements for the conduct of the initial and recertification onsite audit/evaluation, surveillance onsite audits/evaluations (announced and unannounced), onsite special/short notice audits/evaluations for the purpose of complaints investigation, etc. It shall also include provision for examining documentation and records, and access to the relevant equipment and facilities, products, location(s), area(s), personnel, and agency's subcontractors, as needed;

e) The agency shall make claims regarding certification only in respect of the level, location and the scope for which certification has been granted;

f) The agency shall endeavor to ensure that no certificate or report or any part thereof is used in a misleading manner;

g) Keeps a record of all complaints made known to the agency relating to the compliance with certification requirement and to make these records available to the certification body for its verification. The agency shall also agree to take appropriate action with respect to such complaints and any deficiencies found in products/process in accordance with the requirements of the Scheme;

h) The agency shall inform the certification body, without delay, of matters that may affect its ability to conform to the certification requirements. These shall include changes in the:

   i. Legal, commercial, organizational status or ownership, including any changes in its licensing status for provisioning of security services and the Memorandum of Association/Charter having any bearing on private security services.

   ii. Organization and management (e.g. key managerial, decision-making or technical staff),

   iii. Contact address and production sites/premises,

   iv. Modifications in system or processes or the agency operations, changes in in the internal control measures which are significant in nature.

   v. Any other information indicating that the agency may no longer comply with the requirements of the certification criteria and the certification scheme.

2.1.2.2 Records kept by the agency in respect of the complaints received and their resolution shall be verified by the certification body during the surveillance visits to the agency's premises.

2.1.2.3 The agency shall agree for re-audit/evaluation by the certification body as per the requirement of the certification scheme, in the event of changes significantly affecting its capability to comply with the requirements of the certification scheme.

2.1.2.4 The agency shall also agree for re-evaluation by the certification body, in the event of changes in the criteria to which compliance of the private security services is certified.

2.1.2.5 In addition to the requirements as specified above the requirements specified vide clauses 2.5 (confidentiality) shall also be part of the agreement with the client.

2.1.3 Use of license, certificate and marks of conformity - In addition to the requirements as specified in the accreditation standard (clause 8.4 of ISO 17021-1:2015) following requirements shall apply:

2.1.3.1 The certification body shall document clear instructions to clients regarding appropriate use of certification mark(s)/certificate(s) and for providing information about their certification status. It shall also identify the aspects that would be considered as misleading and unauthorised as relevant to the certification scheme. The certification agreement shall make appropriate cross references to the above document, so as to make it legally binding.

2.1.3.2 In case the certification body operates more than one system/product/process certification schemes, then it may document a procedure specifying generic requirements common to all schemes and in line with the requirements of ISO 17021-1:2015 and additional section with specific requirements as specified for the STAR Scheme.

2.1.3.3 Certification mark shall be used only for the security services/offices included in the scope of certification as mentioned on the certificate issued by certification body.

2.1.3.4 The certification body shall have documented procedures for the measures to be adopted in case of non-compliances to specified requirements with respect to use of certification mark, misuse, including false claims as to certification and false use of certification body logo and these shall be part of its agreement with the certified Private Security Agency. The procedure shall include the process steps and the actions (including penal actions as relevant), the certification body intends to take in the event of observing misuse/misleading use of "STARS rating/certification" certificates and certification marks.

2.1.3.5 The certification body shall ensure that the applicants are not misusing the certification mark.

2.2 Impartiality related requirements – In addition to the requirements as specified in clause 5.2 of ISO 17021-1:2015, following requirements shall apply. The requirements as specified below are applicable to the certification levels as specified in clause 1.2 of this document.

2.2.1 The top management's commitment to impartiality shall be demonstrated through:

a) Documenting the certification body's policy on safeguarding impartiality and ensuring that it is understood at all levels of the organization. Implementing good practices like establishing "Code of Conduct" and requiring internal and external personnel to abide by it.

b) Having a defined institutional structure and impartiality policy and procedures, appropriate implementation of these policy and procedures and operation and conduct of its activities and personnel.

c) Having a system that ensures appropriate management of conflict of interest for ensuring objectivity of its certification functions.

d) Taking action to respond to any threats to its impartiality arising from the actions of other parts of the organization, persons outside of the organization, subcontractors, related bodies or other bodies or organizations.

e) Maintaining a professional environment and culture in the organization that supports a behaviour of all personnel that is consistent with impartiality.

f) Making available to public through its website, its policy on impartiality.

2.2.2 The certification body shall not have any relationship with the client except third party conformity assessment. There shall be a minimum separation of 2 years before application can be entertained, in case the certification body has had a relationship with the client which is generic in nature, for example, internal audit, in house training, etc. In cases where the relationship pertained to security services specific activities, then the certification body shall carry out impartiality risk analysis before entertaining the application. The purpose of the risk analysis shall be to ascertain if longer separation than two years is required from the last date of end of relationship as stated above or that the risk is of such unacceptable level so as to prohibit certification by the certification body. Based on the risk analysis, appropriate decision shall be taken and the justification for the same shall be recorded.

2.2.3 If the certification body and its client are both part of government, the two bodies shall not directly report to a person or group having operational responsibility for both. The certification body shall, in view of the impartiality requirement, be able to demonstrate how it deals with a case where both itself and its client are part of government. The certification body shall demonstrate that the applicant receives no advantage and that impartiality is assured.

2.2.4 The certification body shall not outsource/subcontract any part of the certification work, evaluation, marketing, etc, to a legal entity that is engaged in regulatory compliance/processes/services, internal evaluations/audit or training for security services. It shall also not be outsourced to organizations who are engaged in management system consultancy, internal auditing and training and similar services to private security agencies.

2.2.5 When a relationship poses an unacceptable threat to impartiality then certification shall not be provided. Some of these situations requiring prohibitions as mitigation measures have been described vide clause 5.2 of ISO 17021-1:2015. These shall be implemented together with the additional ones provided in this document.

2.2.5.1 In case a related body (Definition of Related Body is based on the relationships as described in Note under clause 5.2.2 of ISO 17021-1:2015) is engaged in any of the activities like management system consultancy, internal auditing or training, then certification shall not be provided to the relevant client to whom these services may have been provided by the related body. There shall be a minimum separation of 2 years, in case the related body has had relationship which is generic (not specific) in nature, for example, internal audit, inhouse training, etc. In cases where the relationship pertained to any services which were security services specific activities, then the certification body shall carry out impartiality risk analysis before entertaining the application. Purpose of risk analysis shall be to ascertain if, longer separation than two years is required from the last date of end of relationship as stated above or that the risk is of such unacceptable level so as to prohibit certification by the certification body. Based on the risk analysis appropriate decision shall be taken and the justification for the same shall be recorded.

2.2.5.2 The certification body shall not certify a Private Security Agency which has received consultancy for regulatory compliance/processes/services, internal evaluations/audit or training, where the relationship between the consultancy organization/individual and the certification body poses an unacceptable threat to the impartiality of the certification body. Allowing a minimum period of two years to elapse following the end of the relationship product consultancy is one way of reducing the threat to impartiality to an acceptable level however, it shall be considered based on the nature of services offered.

2.2.6 All certification body personnel, either internal or external, or committees, who could influence the Private Security Agency certification activities, shall act impartially and shall not allow commercial, financial or other pressures to compromise impartiality. Certification bodies shall require personnel, internal and external, to reveal any situation known to them that may present them or the certification body with a conflict of interests. These aspects shall be ensured through a signed agreement between the individuals and the certification body. Certification bodies shall use this information as input to identifying threats to impartiality raised by the activities of such personnel or by the organizations that employ them, and shall not use such personnel, internal or external.

2.2.7 The certification body's personnel involved in certification activities shall be bound by the certification body's impartiality policy and act impartially in their work through contractual or employment conditions and assignment conditions for each evaluation/audit activity. The certification body shall also take an undertaking with respect to freedom from conflict of interest for every audit/evaluation assignment allotted to the individuals.

2.2.8 The certification body's personnel involved in certification activities shall not provide, while carrying out evaluation/audit, any advice, consultancy or recommendation to the client on how to address any deficiencies that may be identified during the evaluation/audit.

2.2.9 The certification body shall require its personnel, internal and external, to report any situation of influence or pressure from the client that may threaten their independence in the course of certification activities. Based on such report, the certification body shall take appropriate actions to ensure its independence in its certification work.

2.2.10 The certification body shall be responsible for ensuring that neither related bodies, nor sub-contractors, nor internal or external assessors/auditors operate in breach of the undertakings that they have given. It shall also be responsible for implementing appropriate corrective action in the event that such a breach is identified.

2.2.11 The certification body shall ensure that a conflict of interest analysis is carried out in accordance with the requirements specified in clause 5.2.2 of ISO 17021-1:2015, at least once annually and whenever a significant change occurs in the CB's activities, such as changes in the organizational structure and business activities or of the legal status and mergers with, or acquisitions of other organizations. This analysis shall be approved by the impartiality committee (see clause 3.3 of this document) established by the certification body.

2.2.11.1 Further, where risks to impartiality have been identified as a result of risk analysis (clause 2.2.11), the certification body shall establish and implement a documented procedure for mitigation of threats against impartiality. These shall be through any of the following mitigation means:

i. Not provide certification, since the situation poses unacceptable threat to impartiality – prohibition. Some of the prohibitions are already stated in the standard ISO17021-1:2015 and this document.
ii. Carry out the certification in a restricted manner based on disclosures
iii. Minimize the risks on the basis of clearly defined control points to ensure mitigation.

2.3 Liability and financing

2.3.1 In addition to the requirements as specified in clause 5.3 of ISO 17021-1:2015, following requirements shall apply. The requirements as specified above are applicable to all the certification levels as specified in clause 1.2 of this document.

2.3.2 The certification body shall also be able to demonstrate that it has evaluated the risks arising from its certification activities and that it has adequate arrangements (e.g. insurance or reserves) to cover liabilities arising from its operations in each of its fields of activities and the geographic areas in which it operates.

2.3.3 The certification body shall be able to demonstrate that it has a reasonable expectation of being able to provide and to continue to provide the service in accordance with its contractual obligations. Certification bodies shall also be able to provide sufficient evidence to demonstrate its viability, e.g. management reports or minutes, annual reports, financial audit reports, financial plans, etc.

2.3.4 The means by which the certification body obtains financial support shall be such to allow the certification body to retain its impartiality.

2.3.5 In addition to the above the certification body shall also demonstrate to the Impartiality committee, that initially, and on an ongoing basis, commercial, financial or other pressures do not compromise its impartiality.

2.4 Non-discriminatory conditions

2.4.1 The certification body's policies and procedures shall ensure that it does not practice any form of hidden discrimination by speeding up or delaying the processing of applications.

2.4.1 Certification Fees

2.4.1.1 The requirements as specified in clause 13 of the document "Security Agencies Rating Scheme - Certification Process" shall apply.

2.4.1.2 The certification body's fee structure shall be publicly available on its website. The structure shall provide break up of costs.

2.4.1.3 On request from a specific applicant/client, based on the specific conditions concerning the applicant, the certification body shall inform the applicable fees, which shall essentially be derived from the fee structure made publicly available. It shall not substantially differ from the one available publicly, unless some plausible justifications are recorded.

2.5 Confidentiality - In addition to the requirements as prescribed in the accreditation standards (clause 8.5 of ISO 17021-1:2015) following requirements shall apply:

2.5.1 Personnel, including any committee members, contractors, personnel of external bodies or individuals acting on the certification body's behalf, shall keep confidential all information obtained or created during the performance of the certification body's activities. There shall be a mechanism such as obtaining signed confidentiality agreements, etc, for ensuring the same.

2.5.2 The certification body shall have available and use equipment and facilities that ensure the secure handling of confidential information (e.g. documents, records).

2.5.3 When confidential information is made available to other bodies (e.g. accreditation body, agreement group of a peer assessment scheme), the certification body shall inform its client of this action, in advance, through agreements, etc.

2.5.4 In case of transfer of certificate or application, when the client decides to move from one certification body to another certification body, the certification body to which the client is now moving may ask the previous certification body for information on the reasons for such movement or the performance of the client with respect to the certification requirements. The previous certification body shall be obliged to share this information within a reasonable time, not exceeding 10 days from the date of receipt of the request. Such information shall not be considered as confidential and the certification body shall inform its client of this requirement, in advance, through agreements, etc.

2.6 Information Requirements - In addition to the requirements as specified in the accreditation standard (clauses 8.1, 8.3, 8.6 of ISO 17021-1:2015) and the document "Security sTar Agencies Rating Scheme - Certification Process", the following requirements shall apply:

2.6.1 Publicly available information

2.6.1.1 Making the information publicly available through the certification body's website shall be the only means of meeting this requirement.

2.6.1.2 The following information with respect to Security sTar Agencies Rating Scheme shall be made publicly available on the certification body's website. The information provided shall be accurate, non-misleading and where relevant detailed enough for the reader to clearly understand:

a) Information related to the terms and conditions of certification and the use of certificates/certification mark for STAR Scheme, as contained in the Certification Agreement (clause 3 of this document). A description of the rights and duties of applicants and clients, including requirements, restrictions or limitations on the use of the certification body's name and certification mark and on the ways of referring to the certification granted.

b) The CB may also provide any other guidance documents on the certification criteria for the benefit of the applicant, as long as they are not advisory/consultative in nature.

c) The certification body shall make publicly available on its website the information about applications registered and certifications granted, suspended or withdrawn.

d) On request from any party, the certification body shall provide the means to confirm the validity of a given certification and the provision for the same shall be made available on the website.

e) The certification body shall maintain and make publicly available on its website, a directory of valid certifications under "Security sTar Agencies Rating Scheme" scheme that as a minimum shall show the name, relevant certification criteria, Level, scope and geographical locations (e.g. city and country) and contact details for each applicant and certified client and validity of certification for the certified clients. Please also see additional requirements given in the document "Security sTar Agencies Rating Scheme – Certification Process (clause 1.3)", which are required to be placed on the certification bodies website.

2.6.1.3 The certification body shall also make arrangement for providing and up-dating of information with respect to status of certified clients. The certification body shall have procedure for frequent updating of the information on its website. The responsibilities for ensuring accuracy of the information made available on the website, ensuring frequent updates, etc shall be documented.

2.6.1.4 The information on complaints handling process and the certification body's procedure shall be directly available to the public, without the public having to go through layers of cross linkages.

2.6.2 Information exchange between a certification body and its clients

2.6.2.1 Information on the certification activity and requirements- The certification body shall provide and update clients on the following:

a) a detailed description of the initial and continuing certification activity, including the application, initial audit/evaluation, surveillance audit/evaluation, and the process for granting, maintaining, reducing, extending, suspending, withdrawing certification and recertification;

b) the certification/trechnical criteria for STAR scheme;

c) information about the fees for application, initial certification and continuing certification;

d) the certification body's requirements for prospective clients;

e) documents describing the rights and duties of certified clients as well as obligations on part of the certification body including the changes within certified Private Security Agency that need to be informed to the certification body; information on procedures for handling complaints both by the certification body as well by the certified agency, in respect of complaints against certified facilities and appeals;

3. Structural requirements

3.1 In addition to the requirements as specified in clause 6 of ISO 17021-1:2015 following requirements shall apply:

3.2 Organizational structure and top management

3.2.1 The organization structure shall include structure of the parent body (legal entity) if separate from the department/division that offers certification. It shall also include structure of the related departments in relation to the department offering certification services.

3.2.2 The certification body shall identify and document all related bodies (separate legal entities) as well as other departments of the same legal entity and their activities and functions and their relationships with the certification body when describing its organizational structure. This shall cover all relationships and related bodies, bodies related to the certification body based on ownership; governance; management; management personnel; shared resources, finances, contracts and marketing. The activities of all related bodies shall also be documented for the purpose of identifying any potential conflict of interest. The certification body shall also have a system for disclosure and documentation of the types of activities carried out by its internal and external personnel and subcontractors in general and in particular regarding the designing of relevant product/process/service, consultation, internal evaluation/auditing, training, etc. The above information shall also be used for identification of actual/potential risks to impartiality.

3.2.3 The identification of responsibilities, however done, shall clearly and unambiguously reflect the responsibilities for activities/functions as described vide clause 6.1.2 a) to i) of ISO 17021-1:2015.

3.3 Mechanism (Impartiality Committee) for safeguarding impartiality

3.3.1 An Impartiality committee with specific responsibility for safeguarding the certification body's impartiality in its certification functions and for ensuring that the policy on safeguarding impartiality and related procedures and other systems are effectively implemented shall be the only means of fulfilling this requirement. The impartiality committee as specified in clause 6.2 of ISO 17021-1:2015 will fulfil the requirement as specified in this document.

3.3.2 The Impartiality Committee shall:

a) Assist the certification body in developing the policies relating to impartiality of its certification activities,

b) Counteract any tendency on the part of a certification body to allow commercial or other considerations to prevent the consistent objective provision of certification activities,

c) Advise on matters affecting confidence in certification, including openness and public perception,

d) Conduct a review, at least once annually, of the impartiality of the audit, certification and decision making processes of the certification body, and

e) Approve the conflict of interest analysis and the mitigation measures described in clause 2.2.11 of this document.

Other tasks or duties may be assigned to the committee provided these additional tasks or duties do not compromise its essential role of ensuring impartiality.

The composition, terms of reference, duties, authorities, competence of members and responsibilities of this committee shall be formally documented and authorized by the top management of the certification

This committee shall meet regularly, at least once a year, and a complete record of the proceedings of this committee shall be maintained.

3.3.3 The certification body shall ensure that

a) The committee for safeguarding impartiality shall be separated from the management of the certification body operations and established at the highest level within the organization, independent of its day-to-day operations.

b) In the composition of the committee, participation of key interested parties shall be ensured, with a representation of a balance of interests such that no single interest predominates. Internal or external personnel of the certification body are considered to be a single interest, and shall not predominate.

c) Its chairman shall be a person independent from and external to the certification body.

3.3.4 Impartiality Committee meetings may be observed by the Accreditation Body's Assessment Teams as part of the Certification body's accreditation process.

3.3.5 Although every interest cannot be represented in the Committee, a certification body shall identify and invite significantly interested parties. Such interests may include: clients of the certification body customers of organizations whose management systems are certified, representatives of industry trade associations, representatives of governmental regulatory bodies or other governmental services, or representatives of non-governmental organizations, including consumer organizations. The invited representative to impartiality committee shall be some way related to security services field.

4. Resource related and team competence requirements

4.1 In addition to all generic personnel related requirements as specified in clause 7 of ISO 17021-1:2015 following specific requirements shall apply:

4.2 Audit/evaluation team competence

4.2.1 The auditors/evaluators of the certification body carrying out the audit/evaluation of the Private Security Agency against the criteria as described in clause 1.2 above shall have all the following qualifications as described below:

(i) A graduate from a University

(ii) Understanding of PSARA & other applicable statutory and regulatory requirements for Security agencies

(iii) Minimum 2 years work experience in Private Security services sector

(iv) Auditor experience - For a first authorization, the auditor shall comply with the following criteria, which shall be demonstrated in audits under guidance and supervision:

a) For Level 1 to 6 – The auditor shall have gained experience in the entire process of auditing security services quality management systems, including review of documentation, implementation audit and audit reporting. This experience shall have been gained by participation as a trainee in a minimum of two audits for a total of at least 10 mandays under an accredited ISO 9001 programme.

b) Additionally for Level 7 - This experience shall have been gained by participation as a trainee in a minimum of two audits for a total of at least 10 mandays in an accredited ISO 18788 programme,

c) In addition to criteria a) and b) above, the audit team leaders shall have performed as an audit team leader under the supervision of a qualified team leader in at least three ISO 9001 audits for Level 1 to 6 and ISO 18788 audits for Level 7.

4.2.1.1 Additionally for Level 3 and above, the audit team shall have at least one member with a minimum of 3 years Military / Law Enforcement Experience

4.2.1.2 The auditor/evaluator involved in offsite documentation review of information received with the application/ document review before going for onsite assessment shall have the qualifications as described in clause 4.2.1 of this document.

4.2.1.3 The certification body may use ISO 9001 auditors who do not have the requisite qualifications as prescribed above provided they are supported by technical experts (TEs) who meet the qualifications at 4.2.1 above. The time spent by the TE on an audit shall be in addition to the audit time as prescribed under the 'Certification Process' which the CB is expected to spend.

4.2.2 One of the auditors/evaluators in the team shall be nominated as the team leader. The team leader shall be an ISO 9001 Lead Auditor for Level1 to 6 and ISO 18788 Lead Auditor for Level 7, qualified as team leader as per the requirement given in ISO 17021-1:2015.

4.2.3 The certification body will have a system for qualifying lead auditor/evaluators for "Security sTar Agencies Rating Scheme", based on experience of having performed

a) For Level 1 and 2, At least three audits/evaluations under the Security sTar Agencies Rating Scheme at level 1 or Compliance Management System for Security Services. For one time initial qualification, some other evaluation methods such as audit experience as team leader in other technically similar areas may be used.

b) For Level 3 and 4, At least three audits/evaluations under the Security sTar Agencies Rating Scheme at level 3 or ISO 9001 for Security Services. For one time initial qualification, some other evaluation methods such as audit experience as team leader in other technically similar areas or at least five audits/evaluations under the Security sTar Agencies Rating Scheme at level 1 or 2, may be used.

c) For Level 5 and 6, At least three audits/evaluations under the Security sTar Agencies Rating Scheme at level 5 or ISO 9001 for Security Services. For one time initial qualification, some other evaluation methods such as audit experience as team leader in other technically similar areas or at least five audits/evaluations under the Security sTar Agencies Rating Scheme at level 3 or 4, may be used.

d) For Level 7, At least three audits/evaluations under the Security sTar Agencies Rating Scheme at level 7 or ISO 18788. For one time initial qualification, some other evaluation methods such as audit experience as team leader in other technically similar areas or at least five audits/evaluations under the Security sTar Agencies Rating Scheme at level 5 or 6, may be used.

4.2.4 While carrying out audit/evaluation of a Private Security Agency for STARS Technical criteria requirements as specified, the audit team shall collectively have competence as specified in clauses 4.2.1 and 4.2.3 above.

4.3 Other certification body personnel as relevant to the Security sTar Agencies Rating Scheme - Other certification body personnel involved in the scheme certification evaluation activities shall have the competence as stated below:

4.3.1 Application Review personnel – The functions to be carried out by the personnel involved in review of application review is to confirm the adequacy of the information provided by the applicant and identification of the deficiencies observed. Further in case the application reviewer also needs to carry out mandays estimation and team nomination, the persons involved in application review process, shall have thorough knowledge of "Security sTar Agencies Rating Scheme" requirements as defined in this document and "certification process" documents, in addition to meeting the requirements specified in the relevant requirements for application review personnel as specified in ISO17021-1:2015. The application review personnel shall be qualified based on experience of having performed at least three application reviews under the Security sTar Agencies Rating Scheme or through any other equivalent route.

4.3.2 Technical Reviewer – The certification body personnel involved in technical review function shall have the same requirement as that specified in clause 4.2.1 of this document. The technical reviewer shall also meet the qualification criteria as specified in the relevant requirements of ISO17021-1:2015 and shall preferably be qualified on the basis of demonstrated competence to carry out the review function say based on experience of having performed at least three technical reviews under the "Security sTar Agencies Rating Scheme". The technical reviewer shall be independent from the audit/evaluation team.

4.3.3 Decision maker - Any authorized person(s) of the certification body, independent of the persons involved in the evaluation function.

a) The person(s) or committee, who take(s) the decision on granting certification under the STAR scheme, shall have a level of knowledge and experience sufficient to evaluate the information obtained from the evaluation process and the review.

b) The technical review and the decision may be completed concurrently by the same person(s), provided they fulfil the necessary requirements as specified in clause 4.3.2 above and has been specifically authorized for decision making functions.

c) Impartiality and absence of conflict of interest shall be ensured before entrusting the task of certification decision making.

5. Certification Document

5.1 The certificate to be issued to certified Private Security Agency for the options as specified in clause 1.2 of this document shall include the following information:

a) Certificate number

b) Certification scheme name

c) Reference to certification criteria

d) Private Security Agency's name (that of the legal entity) with all permanent locations in the schedule

e) Certified Private Security Agency address

f) Certification Level and Scope of certification

g) Scheme logo

h) logo of the CB

i) Accreditation number with logo

j) Date of certification

k) Expiry date

l) Signature of the CB's authorized representative

In case of Multi Site certification, the CB shall annex to the certificate the list of the certified offices. The temporary sites shall not be included.

6. Complaints and appeals handling system

6.1 All the requirement as specified in clauses 9.7 and 9.8 of ISO 17021-1:2015 are applicable. In addition, the requirements specified below are also applicable.

6.2 In case of complaints related to a certified agency and the services provided by the certified agency, the examination and evaluation of the complaints shall take in to consideration the effectiveness and implementation of the agency's applicable audit criteria (i.e certification level for which agency is certified). The process of establishing validity of the complaint shall generally involve processes like conduct of additional surveillance activities – visit to certified agency's premises for special evaluation, evaluation of the service provisioning process as per implemented system at client sites, if necessary. The decisions on complaint shall then be based on the result of additional surveillance activities.

6.2.1 The certification body's complaint handling process shall document the actions to be taken by the certification body as well as the certified agency, in case the complaint is established to be valid and agency's controls are found to be non- compliant with the specified criteria. Some of these actions/conditions shall also be included in the certification body's legally enforceable contract with the agency.

6.2.2 In respect of appeals, the certification body shall ensure that the individual(s)/committee entrusted with handling of appeal and its resolution/ decision shall be independent of the persons involved in certification related recommendations and decision and their position in the certification body shall be such that it shall not be possible to influence their decisions with respect to the subject of the appeal.

6.2.2.1 The procedure shall also have provision for giving a written statement to the appellant, of the appeal findings including the reasons for the decisions reached and also communicating to the appellant about the provision for giving an opportunity to formally present his case. Based on the presentation made, the individual or a committee appointed for hearing the case shall take a final decision on the appeal and a formal notice of the outcome and the end of the appeal process shall be given to the appellant.

7. Management system requirements

7.1 In addition to the requirements as specified in the accreditation standard (clauses 9.9, 10 of ISO 17021-1:2015) following requirements shall also apply:

7.2 Documentation requirements

7.2.1 The certification body shall document its "Security sTar Agencies Rating Scheme" scheme specific documentation in accordance with the requirements specified in the document "Security sTar Agencies Rating Scheme - Certification Process" and this document, in order to ensure that the certified clients comply with the requirements specified in the Technical Criteria, as applicable.

7.2.2 All applicable requirements of the above document shall be addressed either in a manual or in a combination of manual and associated operational procedures.

7.3 Requirements with respect to records

7.3.1 Records of Applicant and Clients – The certification (applicants and clients) related records shall include records for all Organizations, including all agencies that submitted applications, and all agencies evaluated, certified or with certification suspended or withdrawn/cancelled. Specifically the records shall include the following:

a) Application information and results of application review and mandays estimation and team competence records;

b) Audit/Evaluation planning including decision on site visits in case of multisite certification and preparation records, evaluation plans and other related records;

c) Justification for audit/evaluation time determination/manday estimation

d) Records of initial/surveillance and recertification audit/evaluation reports and related records;

e) Records of verification of correction and corrective actions;

f) Records of technical review and certification decisions; committee deliberations and decisions, if applicable;

g) Certification agreement;

h) Certification Documentation including scope of certification;

i) Records of complaints and appeals, and any subsequent correction or corrective actions;

7.3.2 Other Records – The certification body shall also maintain the following records;

a) Related records necessary to establish the credibility of the certification of STAR Scheme, such as evidence of the competence of auditors/evaluators, technical experts, technical review personnel and decision makers, etc, as relevant;

b) Any other records as relevant to the "Security sTar Agencies Rating Scheme - Certification Process", in order to provide confidence that the scheme requirements were complied with.

7.4 Internal audit – following additional requirements shall be applicable:

7.4.1 The objectives of the internal audit shall also include verification of fulfilment of requirements of the additional STAR Scheme specific requirements as specified in "Security sTar Agencies Rating Scheme - Certification Process" and this document.

7.4.2 The audit program shall cover all applicable elements of ISO 17021-1:2015 and those specified in "Security sTar Agencies Rating Scheme - Certification Process" and this document.

7.4.3 The internal audit shall be conducted by personnel knowledgeable in certification, auditing and the requirements of ISO 17021-1:2015 and the scheme specific requirements as specified in "Security sTar Agencies Rating Scheme - Certification Process" and this document.

7.4.4 The internal audit report shall clearly report both the compliance (to the requirements specified vide clause 7.4.1 above and the certification bodies own systems) aspects as well as the observed gaps (non-conformities), areas for improvement, along with the objective evidences to support the conclusions drawn.