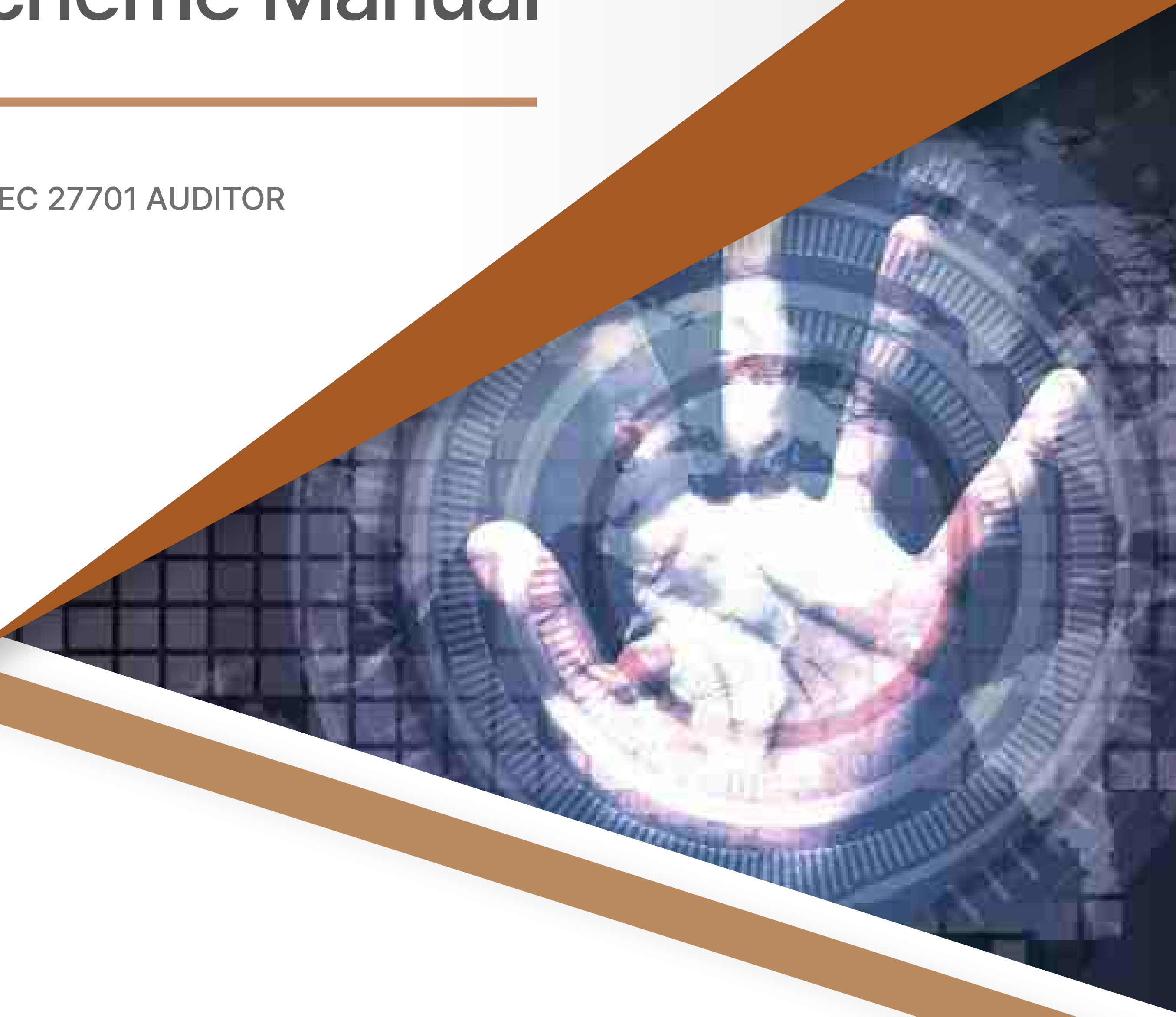
Certification
Scheme Manual

ISO/IEC 27701 AUDITOR



Global Personnel Certification
Rm 501-1, Daeryung techno town, 638,
Seobusaet-gil,Geumcheon-gu, Seoul, Korea

Tel: +82 2 6749 0710
Fax: +82 2 6749 0711
E-mail: info@gpcert.org

www.gpcert.org

CONTENTS

01 Code of Conduct

The Code of Conduct of GPC sets out the standards for GPC certified auditors to meet the requirements for their behaviors and ethics.

By agreeing to the below Code of Conduct, you will demonstrate the required standard as GPC certified auditor.

1) GPC auditors should perform activities in a professional, accurate, and unbiased manner. They should be applied for professional skill and judgement to the best auditing at all times.

2) GPC auditors should develop their own professional competence and maintain their best status for correct auditing.

3) GPC auditors should avoid any involvement which rise to conflict of interest.

4) GPC auditors should not act in any way of prejudicial method to the reputation, interest and credibility of the GPC.

5) GPC auditors should not disclose the findings, information or any part of them gained in the course of the audit unless authorized in writing by both the auditee and the GPC to do so.

6) GPC auditors should not accept any commission, gift or other benefit from organizations being audited, their employees or interested parties.

7) GPC auditors should not intentionally communicate false or misleading information that may compromise the integrity of any audit or the auditor certification process.

8) GPC auditors should take care not to publish or otherwise communicate unjustified and unreasonable criticism of another members auditing work.

9) GPC auditors should not breach any part of this Code of Conduct and provide full cooperation in any formal enquiry that requested to keep the Code of Conduct from GPC.

02 Scope of Certification Auditor Grade

1) Internal Auditor

Management system internal auditor is defined as a person who has been approved by GPC and can perform audit activities as a member of the audit team during internal audit.

2) Provisional Auditor

Management system provisional auditor is defined as a person who has been approved by GPC and is qualified to assist audit activities as a member of the audit team.

3) Auditor

Management system auditor is defined as a person who has been approved by GPC and can perform audit activities as a member of the audit team.

4) Lead Auditor

Management system lead auditor is defined as a person who has been approved by GPC and can perform audit activities as the audit team leader.

5) Senior Auditor

Management system senior auditor is defined as a person who can perform the evaluation by attending the on-site audit in order to evaluate the competency of the auditor certification applicant after receiving approval through a separate approval procedure by the lead auditor approved by GPC.

03 The Requirements for Auditor Certification

1) Internal Auditor

- Professional education or training to an equivalent level of university education
- Work experience of 3 years in the field of information security (including at least 1 years of work experience in the field of privacy information)
- Successful completion of ISO/IEC 27001:2013 and ISO/IEC 27701:2019 Auditor training or internal auditor training
- Internal audit log of at least 5 times, at least 15M/D within the last 3 years
- Pass knowledge and attribution examination of GPC

2) Provisional Auditor

- Professional education or training to an equivalent level of university education
- Successful completion of ISO/IEC 27001:2013 and ISO/IEC 27701:2019 Auditor/Lead Auditor training
- Pass knowledge and attribution examination of GPC

3) Auditor

- Professional education or training to an equivalent level of university education
- Work experience of 4 years in the field of information security (including at least 2 years of work experience in the field of privacy information)
- Successful completion of ISO/IEC 27001:2013 and ISO/IEC 27701:2019 Auditor/Lead Auditor training
- Audit log of at least 20 M/D within the last 3 years (including On-site audit log of at least 8M/D and audit log of at least 3 times)
- Pass knowledge and attribution examination of GPC

4) Lead Auditor

- Professional education or training to an equivalent level of university education
- Work experience of 4 years in the field of information security (including at least 2 years of work experience in the field of privacy information)
- Successful completion of ISO/IEC 27001:2013 and ISO/IEC 27701:2019 Auditor/Lead Auditor training
- Audit log of at least 35 M/D within the last 3 years (including audit log of at least 15M/D as a team leader and On-site audit log of at least 8M/D and audit log of at least 3 times)
- Pass knowledge and attribution examination of GPC

5) Senior Auditor

- Professional education or training to an equivalent level of university education
- Work experience of 10 years in the field of information security (including at least 5 years of work experience in the field of privacy information)
- Maintaining the certification as a lead auditor at the current accredited PCB
- Audit log of at least 15 M/D as a lead auditor within the last 3 years performed after holding the lead auditor certification at an accredited PCB (including On-site audit log of at least 8M/D and audit log of at least 3 times)
- Pass knowledge and attribution examination of GPC

6) Detailed requirements

- Education

  University graduation or higher is required. Applicants must provide proof of their final academic background.

- Work experience

  Work experience in information technology (IT) is required, including work experience in privacy information.

Privacy information related work experience includes:

a. Implementation of privacy information management system
b. A member of a team in charge of privacy information

For any other experience other than ISO/IEC 27701 related or work experience in the privacy information field, the acceptance will be decided after review of the supporting materials. (Example: consulting, etc.)

- Auditor training course

After completing the auditor/lead auditor training course, the auditor/lead auditor transition course, or the auditor/lead auditor expansion course conducted by an accredited PCB or a training provider designated by it, applicant should pass the GPC knowledge and attribution examination. If it is not a training certificate issued by an accredited PCB or a training provider designated by it, applicant should submit evidence that can prove the effectiveness and validity of the training course. For the auditor/lead auditor training course, it must be a minimum of 5 days (40 hours), and for the auditor/lead auditor transition course or the auditor/lead auditor expansion course, it should be a minimum of 2 days (16 hours). However, only training certificates within 3 years from the date of application can be accepted.

- Audit log

All of the 1st, 2nd and 3rd party audits are recognized as the log of audit. Initial, surveillance, and recertification audits are all accepted, and at least one initial audit must be performed.

It is possible to accommodate up to 5M/D per audit of one time.

(If an applicant performed 7 M/D audit in one time, it is calculated as 5 M/D.)

In the case of similar audit log related to ISO/IEC 27701, it should be equivalent to the ISO/IEC 27701 standard to be recognized as the audit log, and applicant should submit the data on the criteria applied to the similar audit for equivalence evaluation.

04 Examination

1) Type of examination

- Knowledge exam

  exam to evaluate the knowledge of the applied ISO standard

- Attribution exam

  exam to evaluate whether the subject of evaluation has basic auditor qualifications and attitude

2) Criteria of pass

a) Knowledge exam

The knowledge exam has a total of 50 questions and consists of 4 sections divided.

Each question is allotted two points, and the pass criterion is 70 points.

* Even if the total points are more than 70 points, the applicant cannot pass the exam without the minimum points required for each section. (More than 40% of correct answers per section)

Time limitation is only 60 minutes for the examination, and it is open-book (Received Hard copied standard from GPC) condition.

If one is failed in the exam, candidate is given one more chance of examination. If candidate fails to the consecutive examination, the candidate may not retake the exam for one year.

b) Attribution exam

The purpose of the attribution exam is to evaluate the characteristics and the qualification as an auditor, and it asks how much the application understandable agree with the questions.

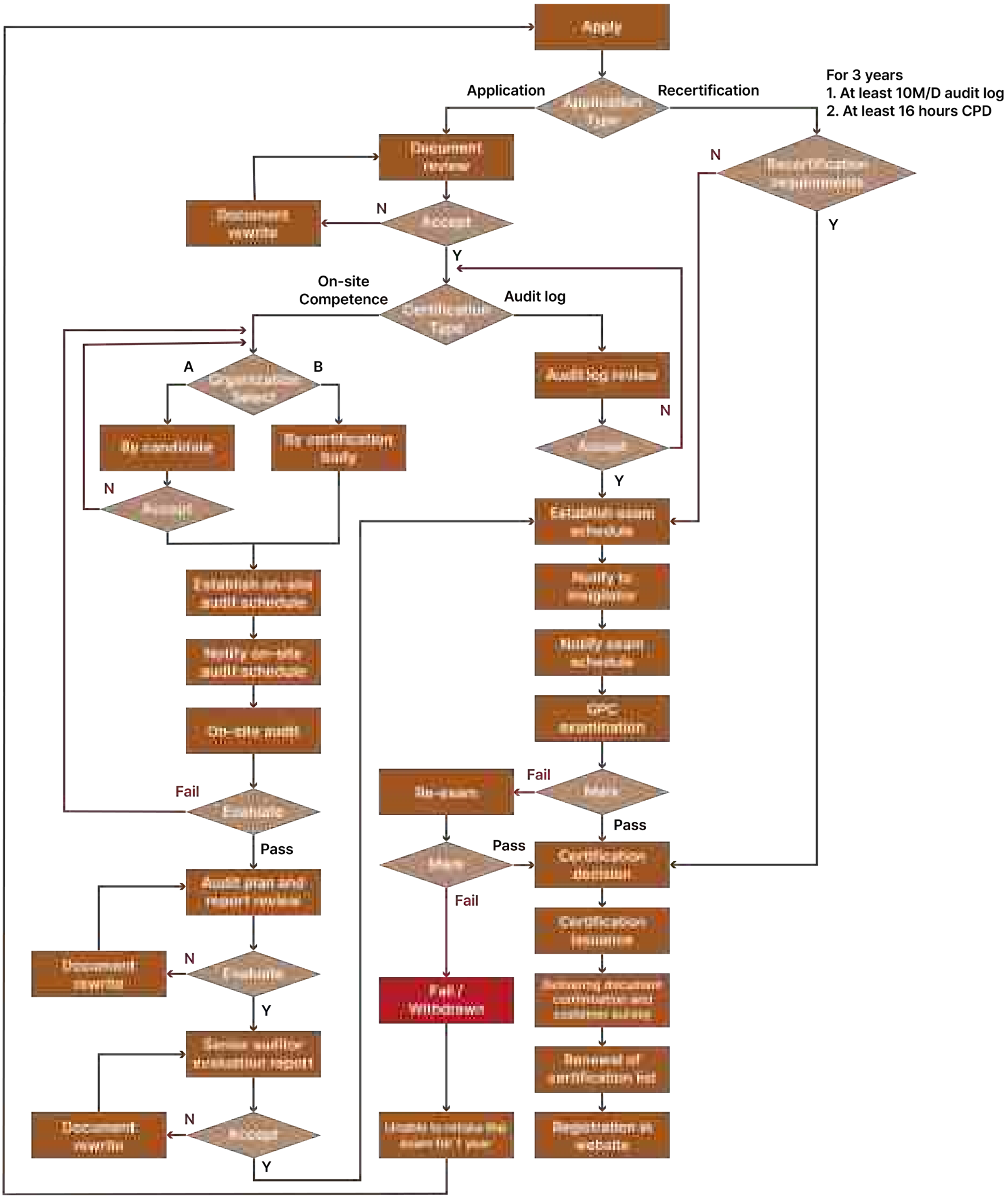
It is based on ISO 19011:2018 and consists of 25 questions only. The candidate should choose the answer that comes to mind first.

Up to 4 points are given for each question and as the answer is further from the correct answer, 1 point each is deducted. (0 point for no answer)

Time limitation is only 30 minutes for the examination, and the pass criterion is 70 points.

If one is failed in the test, another chance of attribution re-examination (written test) is given. If candidate fails to the attribution re-examination, the candidate may not retake the exam for one year.

05 Certification Process



06 Surveillance and Re-certification Process

1) Surveillance

- It is required at the annual maintenance fee without special requirements.

2) Re-certification

- For all grades, recertification applications must be made every three years from the date of initial issue and must be carried out within a period of around six months from the expiration date.

  As evidence required for grades excluding the provisional auditor and internal auditors, an audit log of at least 10M/D for 3 years (at least 3 audit times) and a record of CPD (Continuing Professional Development) of 16 hours or more should be submitted.

  (CPD activities must be demonstrated by materials that are acceptable for training, seminars, workshops, or other professional development activities.)

- Internal auditors are required to have an internal audit log of at least 3M/D for 3 years (at least 3 audit times).
- In the case of a lead auditor, an audit log is required as at least one of lead auditor additionally.
- In the case of a senior auditor, at least one audit log as a lead auditor and on-site competence evaluation activity are additionally required.

07 Suspension and Withdrawn Process

1) Suspension

a) Reason of suspension

- When the requirements for maintaining certification or re-certification are not met
- When the customer does not apply for re-certification
- When there is a customer's request for suspension
- When the customer does not pay the certification fee
- When the auditor’s Code of Conduct is violated

b) Suspension may be withheld if appropriate action is taken within 15 days of the occurrence of the cause of the suspension.

c) The period of suspension can not exceed six months.

d) Auditors who have been suspended from certification may not immediately use documents certification, marks of GPC and accreditation body, etc.

e) If the cause of the suspension is resolved, the certification can be restored after approval by GPC.

2) Withdrawn

a) Reason of withdrawn

- When the requirements for maintaining certification or re-certification are not met
- When the customer does not apply for re-certification
- When the problem causing the suspension is not resolved within 6 months of the period set by GPC
- When the customer does not pay the certification fee within the expiration period
- When the customer requests withdrawal
- When the auditor’s Code of Conduct is violated

b) GPC will review and accept the customer's action if appropriate within 15 days.

c) GPC will withdraw the certification if it does not respond within 15 days or does not take appropriate action.

d) The customer should immediately stop using the certification documents and marks.

e) If the customer wants to re-certify, GPC will proceed with the new certification.

f) When a customer reapplies for a withdrawn certification, GPC ensures that the reason for withdrawn has been resolved by recording the confirmation in the remarks section of the application.

08 Appeals and Complaint Process

1) Appeals Process

Any client can take issue as an appeal against the GPC decision on certification. The appeal against the decision of GPC must be made within 30 days of notification of that decision.

The appeals can be submitted to the GPC Administration department, along with evidence materials, to the email address below.

mail: info@gpcert.org

The administration department should check the documents for completeness and may ask for additional documentary, if necessary. After checking the appeal should be forwarded to the manager of administration department. The manager has the right to either disallow the appeal or to organize an Appeal Panel based on the contents of the appeal.

An appeal against adverse certification or recertification decisions or cancellation of certification should be treated in writing form. The written appeal will be reviewed, investigated and resolved in a timely manner through a formal documented process. Appeals can be processed on the following decisions:

a. Refusal to grant initial certification
b. Refusal to grant continual certification
c. Refusal to grant upgrade certification
d. Reduction in certification grade

If the appeal is accepted, manager of administration department will organize an Appeal Panel. The Head of the Appeal Panel may ask the appellant to present, if necessary.

The Appeal Panel gives its recommendation to the manager of administration department for necessary action to discharge the appeal to the satisfaction of the appellant. The Appeal Panel also recommends preventive action, if any, to avoid such recurrences. The manager of administration department will give the decision on the appeal based on the recommendation by the appeals panel. The decision of the manager of administration department will be final.

The above process will be completed within 45 days from the date of admission to the appeal.

If not satisfied with the decision of the manager of administration department, appellant can file appeal to the President of GPC. The president will organize Appeal Panel consisting of three members, that will go into the situation of the case and the procedure follows to address the appeal.

The Appeal Panel will make recommendation to the president. The president will give the decision based on the recommendation by the appeal panel. The above process will be completed within 45 days of referring the appeal to the president. The president shall be acting on the advice of any appropriate specialist, if necessary.

If the appeals ends or a reassessment or verification is required as a result of the appeal decision, the cost of the appeal is borne by the appellant.

If not satisfied with the decision of the President of GPC, the appellant can file appeal to the Accreditation Body. However, this process is only possible after all processes have been taken to resolve the issue by filing appeal with GPC. In such a case, the Accreditation Body's appeals process shall be followed, and the costs of appeal shall be borne by the appellant unless the appeal is accepted. The decision of the relevant Accreditation Body shall be final and binding on both parties, i.e., the appellant and GPC. Administration department maintains the track of the appeals, including action taken to resolve them. In the event of a dispute, the laws and regulations of the Republic of Korea where GPC is located will apply, and Court of Korea can have full control over administrative process.

2) Complaint Process

Complaints are handled by administration department. Administration department has the authority to receive, verify and investigate complaints and to make corrective actions for complaints.

A written and/or verbal, external as well as internal complaints can be received by any employee/staff of GPC.

The complaint received shall be forwarded to manager of administration department, who will immediately enter it into the complaints register being maintained at GPC. Additional information may be requested from the complainant, if necessary.

The complaint shall be acknowledged within 24 hours of receipt by telephone or by sending an e-mail. If possible, formal notice shall be given to the complainant about the end of the complaint handling process.

Manager of administration department will forward the complainant to the concerned official of GPC for disposition, who will take necessary corrective and preventive action to close the complaint, without any undue delay.

The result of handling complaint shall be communicated to the complainant. The complainant and the content of the complaint shall be kept confidential in accordance with GPC complaint handling procedure.

09 Knowledge Requirements

The ISO/IEC 27701 auditor should understand the requirements for ISO/IEC 27701 and the relationship between those requirements and have the following knowledge required by ISO/IEC TS 27006-2:

a) Privacy information management including ISO/IEC 27701

b) Identification and handling of personally identifiable information (PII)

c) Privacy by design and by default

d) PIMS monitoring, measurement, analysis and evaluation

e) Information security risks related to privacy information management and processing of PII

f) Policies and business requirements for privacy information management

g) Privacy information management and processing of PII related tools, methods, techniques and their application

h) Tracing privacy incidents

i) Privacy information risk assessment, privacy impact assessment and the related methods and risk management

j) Processes applicable to PIMS

k) The current technology where privacy may be relevant or an issue

l) All controls contained in ISO/IEC 27701 and their implementation

m) The legal requirements that apply to privacy information management and/or processing of PII

n) Industry privacy good practices and privacy procedures

Certification Scheme Manual

GLOBAL PERSONNEL CERTIFICATION

Company name : Global Personnel Certification **Address** : 501-1, 638, Seobusaet-gil, Geumchoen-gu, Seoul, Republic of Korea
TEL : 02) 6749-0710 **Fax** : 02) 6749-0711 **E-mail** : info@gpcert.org **www.gpcert.org**