1.0 TITLE: Auditing Procedure

2.0 PURPOSE: To provide an outline and instructions on the GMCS auditing process of clients.

3.0 RESPONSIBILITY: GMCS auditors and personnel and GMCS clients are responsible for following this procedure.

4.0 SCOPE: This procedure applies to all third-party audits conducted by GMCS. GMCS client organizations should be aware that when accredited certification is chosen by a client, requirements outside of the management system standard exist which impact and affect GMCS and GMCS client procedures, processes, practices, and record keeping. The International Accreditation Forum (IAF), International Accreditation Service (IAS), and GMCS each have standards, procedures, guidelines, and requirements which exist outside of the management system standard which affect the certification process.

5.0 QUALITY OBJECTIVE: To issue the Audit Report to the client at the Closing Meeting.

6.0 REFERENCE DOCUMENTS: ISO 17021 Manual, ISO 9001, ISO 14001, ISO 45001, ISO/IEC27001, ISO/IEC 20000-1, ISO 13485, ISO 19011, IAF MD 5, IAF MD 17, IAF MD's, IAS Procedures, MSA-01

7.0 PROCEDURE:

A. The President of GMCS is responsible for reviewing all Applications for Certification and Applications for Transfer of Certification (Note: a majority of GMCS clients are the US government and military. The Solicitation for certification services along with the GMCS Technical Proposal and Pricing Proposal will function as an adequate substitute for a formal application and the completion of GMCS Application of Registration GMCS-APPAR-01 and the GMCS Review of Customer Requirements Form GMCS-RCR-01).

The President will complete the Review of Customer Requirements on Form RCR-01 for all clients excluding government and military clients. This Form will indicate the specific IAF Codes applicable to the Client for QMS, EMS, or other management system standards. The Table containing the Codes has been color coded as follows: No Color=the Code is within GMCS current scope of accreditation, Blue=the Code is non-critical and not within the GMCS current scope of accreditation, and RED=the Code is critical and not within the current scope of accreditation. The Codes selected

1200 G Street, NW, Suite 800
Washington, DC 20005
(202) 351-6837

will determine whether IAS must witness the audit or not and whether the Codes selected are Critical or not.

B. After accepting any such application or being awarded a government/military contract, the President is responsible for appointing a Lead Auditor and additional auditors, if necessary, to conduct the audit of the client's management system. In making such appointments, the President follows the requirements stated in the GMCS ISO 17021 Manual (Section 7.1.2). The Audit Team must collectively have experience with the Client's industry and IAF Code(s). Unless there is only one auditor, no one auditor is required to have experience with all IAF Codes identified by the client.

C. The President is responsible for communicating to the Lead Auditor the type of audit that needs to be conducted (e.g. Stage 1, Stage 2, Surveillance, etc.) and for providing all relevant information and documentation to the Lead Auditor (e.g. documented scope, policy, objectives and procedures, sites to be audited, audit duration, etc.). This information is provided on a Customer Data Sheet (CDS).

D. The Lead Auditor is responsible for communicating with the GMCS client, establishing authority to conduct the audit, making all necessary logistical arrangements, and submitting the draft Audit Plan and Schedule (GMCS-AP-001).

E. Standards-GMCS requires that its clients own a licensed copy of any management system standard for which it is seeking certification along with any supporting standards referenced in the specification standard. For example, Organization X is seeking to become ISO 9001 certified. It must own a licensed copy of ISO 9001, ISO 19011, and ISO 9000. The best source for any ISO standard is www.iso.org

F. Scope and Certificate of Certification-All management system standards require a documented scope. The term "scope" means physical boundaries, processes, organizational business units, areas of a management standard which do not apply to the organization, and complexity and risk levels for certain standards such as ISO 14001, ISO/IEC 27001, and ISO 45001.

All GMCS clients must have a documented scope which includes the following information precisely and accurately stated: 1) organizational name (specifically stated (e.g. if a business unit or division within a larger entity is pursuing certification, then a tiered description must be stated), 2) physical (not mailing) address (including, where appropriate, floor number(s), and/or building number(s), process names, areas of non-applicability, and where applicable, risk and complexity level stated (see IAF MD 5). Clients are advised to review the applicable section

1200 G Street, NW, Suite 800
Washington, DC 20005
(202) 351-6837

requiring a documented scope in the Management System standard along with any associated standards (e.g. ISO 9001 Section 4.3, ISO 9000 Section 3.13.5, ISO 19011 Section 6.2.2). In addition, ISO 17021 governing all accredited Certification Bodies Section 8.2.2 and the ISO and IAF Auditing Practices Group (APG) provides further guidance and requirements on management system scope. The GMCS Certificate of Conformance shall list the sub scopes for each site as stated in the Client's documented scope of its Management System and as verified by GMCS. Temporary sites shall be identified as temporary on the Certificate. Temporary sites shall be identified as temporary on the Certificate. When the Client updates the scope statement, the revised scope statement MUST be sent to GMCS at the time the revision has been approved with the Client's organization. Failure to submit the revised scope at the time the revision in made will result in a documented nonconformance.

Some individuals are under the impression that a Certification Body (CB) can put whatever it wants on a Certificate of Conformance. In fact, a CB must use the documented Scope when generating a Certificate. The Scope statement drives the information on the Certificate and not the other way around. There is a pervasive issue globally with organizations misrepresenting the depth and breadth of their certification.

The documented scope should be brief and should refrain from including additional information such as background and history of the organization or any additional information other than the requirements stated above.

Caution: Military clients, in particular, should be aware that their locations may house tenant activities and contractor (GOCO) managed activities which may or may not be a part of the scope of the management system standard. It is imperative that the documented scope statement address this issue as well. For ISO 14001 and ISO 45001 clients, tenant agreements must specifically address whether the tenant is a part of the SMS and/or EMS (and typically do so even without ISO 14001 or ISO 45001 certification). When such an agreement states that the tenant is a part of the EMS and/or SMS, then the scope must include these tenant activities. Contracts with Contractors often state that the Contractor must comply with the customer's EMS and/or SMS. When this is the case, the Contractor and its activities must be included in the scope of the EMS and/or SMS (see Appendix of ISO 14001 and ISO 45001 for further information).

For ISO 13485 clients, GMCS shall precisely document the scope of certification. GMCS shall not exclude part of processes, products, or services (unless allowed by regulatory authorities) from the scope of certification when those processes,

1200 G Street, NW, Suite 800
Washington, DC 20005
(202) 351-6837

products or services have an influence on the safety and quality of products (see IAF MD 9, Section 8.2).

G. Policy-All management system standards require a documented policy be issued from top management (e.g. ISO 9001-Quality Policy, ISO 14001-Environmental Policy, etc.). GMCS clients are cautioned to ensure that: 1) the Policy contains the commitments as stated in the Management System Standard-deviating from the language of the requirement often results in a change in the meaning and the intention of the Standard which is a nonconformance, and 2) the length of the Policy should be considered since all Policies must be communicated and understood by personnel (employees and contractors) working within the scope of the management system. It is difficult to ensure that these personnel understand such a Policy when the Policy is lengthy.

H. Objectives-All Management System standards require the establishment of measurable goals and objectives. GMCS will review these goals and objectives to ensure that they are measurable, measured, and relevant to the Standard being assessed (e.g. ISO 9001 requires quality objectives so documenting safety objectives would not be relevant). Goals and objectives which are always met or never met are useless and do not drive continual improvement.

I. Management Review-All Management System standards require top management review the Management System at planned intervals. The minimum accepted interval for review is once per calendar/fiscal year whereby all required inputs and outputs have been reviewed. Typical evidence presented includes attendance records, agendas, and minutes. The definition of "top management" can be found within each standard or for ISO 9001 clients in ISO 9000.

J. Internal Audits-Internal auditing is a common requirement of all Management System standards. GMCS will review the internal audit program including audit plans and schedules, audit reports, audit checklists, and corrective actions. Management system standards require these internal audits be performed at "planned intervals" without stating the interval. GMCS requires an interval of no less than once every three years coinciding with the period of certification. All requirements of the Management System standard (unless there are areas of non-applicability) and all processes must be audited during this minimum interval. Clients are encouraged to develop an interval that is appropriate after assessing risk.

K. Calibration and Metrology-For ISO 9001 clients that maintain equipment requiring calibration (see ISO 9001 Section 7.1.5.2) (i.e. calibration of Test Measurement and Diagnostic Equipment (TMDE)), GMCS clients must use an ISO 17025 accredited metrology

1200 G Street, NW, Suite 800
Washington, DC 20005
(202) 351-6837

lab to ensure traceability to US national standards (i.e. NIST) or international standards. Traceability is not a requirement for ISO 14001 or ISO 45001 although it is recommended.

When choosing a metrology lab, GMCS clients should obtain a copy of the metrology labs ISO 17025 Certificate of Accreditation and ensure that the equipment being sent to the laboratory is stated within the scope of accreditation along with the ranges for that equipment. A Certificate of Accreditation to ISO 17025 does not cover all test, measurement, and diagnostic equipment. In addition, an ISO 17025 accredited metrology laboratory is permitted to issue unaccredited certificates of calibration to its clients. GMCS clients are solely responsible for ensuring that all certificates obtained from a metrology laboratory contains the Accreditation Body (AB) mark. The absence of this Mark means the certificate is unaccredited.

GMCS clients must notify the metrology laboratory that they require ISO 17025 accredited certificates with their equipment when it is returned, and that Accreditation Body logo must appear on the Certificate of Calibration.

TMDE that is used for non-precision measurement and testing (e.g. a “go, no-go”, “is there pressure or no pressure”, etc.) does not require calibration. However, it must have a clear indicator on the device indicating that calibration is not required (e.g. “CNR”).

GMCS auditors will verify these issues during audits, where applicable.

NOTE: Some US government and military calibration laboratories may have ISO 17025 compliant systems that will meet these requirements (e.g., US Army USATA).

L. Consultants-GMCS recognizes that many organizations will use a consultant or consulting firm to set-up their Management System. GMCS prohibits such Consultants from participating in GMCS certification or surveillance audits including acting as Observers during such audits. GMCS expects its clients to have an effective Management System which means that the client (and not the Consultant) can demonstrate that the System is used and effective. Note: Some US government and military organizations will have consultants embedded within their organization as contracted FTE’s. These individuals can be involved in the certification process and GMCS audits.

M. Opening and Closing Meetings-All audits will include an Opening Meeting and a Closing Meeting. The topics covered will follow the topics stated in ISO 19011. For audits occurring over multiple days and/or multiple sites, a daily out brief will be held, and the opening meeting will be conducted on the first day of the audit and the closing meeting

1200 G Street, NW, Suite 800
Washington, DC 20005
(202) 351-6837

will be conducted on the last day of the audit. For ISO 45001 clients, IAF MD 22, requires that your organization's representative shall be requested to invite the management legally responsible for occupational health and safety, personnel responsible for monitoring employees' health and the employees' representative(s) with responsibility for occupational health and safety to attend the closing meeting. Justification in case of absence shall be recorded. Attendance is taken for all Opening and Closing Meetings.

M. Preassessment-A preassessment (aka "Mock Certification Audit") is not a required service to achieve certification. However, clients may elect to have a preassessment conducted to determine their readiness for certification. A preassessment audit report is issued to a client and can be used by the client to address deficiencies in the Management System and to prepare for the Stage 1 and 2 audits.

N. Stage 1 Audit- When a Stage 1 audit is required, GMCS conducts an assessment both onsite at the client's facility (for newly certified clients-not for recertification or new clients who have a valid, current, and accredited certificate and are transferring their certification to GMCS) and offsite of the Management System Manual, if any, and basic fundamental management system processes and procedures including: Management Review, Internal Audits, Control of Documented Information, Corrective Action, Scope, Policy, and Objectives. GMCS's office is responsible for reviewing these fundamental processes and procedures and verifying that each has been documented in accordance with the specification Standard. The GMCS auditor is responsible for verifying that the procedures and documents have been effectively implemented by the organization during the onsite audit. In addition, GMCS ensures that the scope, size of the organization, and the information provided by the Client to GMCS in the Application for Certification is accurate, true, and correct. The Stage 1 audit must occur both on and off site at the client's facility. The results of the Stage 1 Audit are documented on the Stage 1 Audit Report. The format and document number for the Stage 1 Audit Report is dictated by the specification standard. In the event that the Stage 1 Audit results indicate that these general processes and procedures have not been effectively implemented, the client will have up to six (6) months to effectively implement corrective action(s) at which time GMCS will verify the effectiveness of such corrective action(s) and will continue with the Stage 2 audit. If more than six (6) months has lapsed since the Stage 1 Audit was completed, GMCS will require the Client to repeat the Stage 1 Audit. These checklists become a part of the Certification Committee package. Nonconformances discovered during the Stage 1 audit are documented on the Documentation Review Report along with the client response. GMCS does not use the Client Corrective Action Form to document nonconformances cited during a Stage 1 Audit.

1200 G Street, NW, Suite 800
Washington, DC 20005
(202) 351-6837

O. Stage 2 Audit-GMCS conducts a Stage 2 audit to evaluate the effectiveness of the client's management system. Stage 2 audits take place onsite at the client's facility. The timeframe between Stage 1 and 2 shall not exceed six (6) months. If this timeframe is exceeded, the Stage 1 audit shall be repeated. The following items are assessed at a minimum:

a) information and evidence about conformity to all requirements of the applicable management system standard or other normative document;

b) performance monitoring, measuring, reporting and reviewing against key performance objectives and targets (consistent with the expectations in the applicable management system standard or other normative document);

c) the client's management system and performance as regards legal compliance;

d) operational control of the client's processes;

e) internal auditing and management review;

f) management responsibility for the client's policies.

g) links between the normative requirements, policy, performance objectives and targets (consistent with the expectations in the applicable management system standard or other normative document), any applicable legal requirements, responsibilities, competence of personnel, operations, procedures, performance data and internal audit findings and conclusions.

The Stage 2 Audit must utilize the Audit Plan (GMCS-AP-01), Opening Meeting Agenda (GMCS-OMA-01), Closing Meeting Agenda (GMCS-CMA-01), Opening and Closing Meeting Attendance Record (GMCS-AAR-01), Corrective Action Request (GMCS-CAR-01), if applicable and Audit Report The Audit Plan, Audit Report, Corrective Action Request, and Opening and Closing Meeting Attendance forms when completed must be sent to the President for review.

The results of the Stage 2 Audit are recorded on the appropriate GMCS Audit Report. Checklists must be used and GMCS auditors must each complete this Checklist. In the event that there is more than one site being audited, each auditor is required to complete a separate Checklist for each site they audit OR they must ensure that the

1200 G Street, NW, Suite 800
Washington, DC 20005
(202) 351-6837

single checklist they use clearly annotates the fact that both sites have been audited against specific requirements. The checklists may originate from the auditors.

P. Surveillance-After certification is granted to a Client, GMCS will conduct a surveillance audit at a 6- or 12-month interval. Surveillance audits will be conducted at least once a calendar year. The date of the first surveillance audit following initial certification will not be more than 12 months from the last day of the stage 2 audit.

The purpose of the surveillance audit is to ensure that the management system has been sufficiently maintained. Each surveillance audit will review the following management system requirements: a) internal audits and management review, b) a review of actions taken on nonconformities identified during the previous audit, c) treatment of complaints, d) effectiveness of the management system with regard to achieving the certified client's objectives, e) progress of planned activities aimed at continual improvement, f) continuing operational control, g) review of any changes, and h) use of marks and/or any other reference to certification.

All Surveillance Audits require the use of the Audit Plan (GMCS-AP-01), Opening Meeting Agenda (GMCS-OMA-01), Closing Meeting Agenda (GMCS-CMA-01), Opening and Closing Meeting Attendance Record (GMCS-AAR-01), Corrective Action Request (GMCS-CAR-01), if applicable, and Audit Report. The Audit Plan, Audit Report, Corrective Action Request, and Opening and Closing Meeting Attendance forms when completed must be sent to the President for review. The President will review the records and determine whether maintenance of the certification is warranted. Records of all surveillance audit activities are maintained in accordance with the GMCS Control of Records Procedure.

When conducted annually, surveillance audits will always review: Management Review, Internal Audits, Corrective Action, Customer Complaints, Objectives, Scope, and Policy. These items will be reviewed once per calendar year when audits are conducted semi-annually.

For ISO 13485 clients, the surveillance program shall include a review of actions taken for notification of adverse events, advisory notices, and recalls (see IAF MD 9, Section 9.6).

Q. Recertification-The purpose of the Recertification Audit is to evaluate the continued fulfillment of all of the requirements of the relevant management system standard or other normative document and to confirm the continued conformity and effectiveness of the management system as a whole, and its continued relevance and applicability for the scope of certification. A recertification audit

1200 G Street, NW, Suite 800
Washington, DC 20005
(202) 351-6837

should occur sixty (60) days prior to the expiration of a Certificate to ensure that there is no lapse in certification. A recertification audit which occurs MORE THAN sixty days before expiration will result in a reset of the 3-year period of certification and will truncate the existing period of certification.

Recertification audits consider the performance of the management system over the period of certification, and include the review of previous surveillance audit reports. When significant changes to a Client organization have been discovered, it may be necessary to conduct a Stage 1 audit as part of the recertification process. If the client has multiple sites or multiple management system standards, GMCS will ensure that sufficient time is provided to ensure that a thorough assessment is undertaken and that GMCS has confidence in the audit process.

All Recertification Audits require the use of the Audit Plan (GMCS-AP-01), Opening Meeting Agenda (GMCS-OMA-01), Closing Meeting Agenda (GMCS-CMA-01), Opening and Closing Meeting Attendance Record (GMCS-AAR-01), Corrective Action Request (GMCS-CAR-01), if applicable, and Audit Report. The Audit Plan, Audit Report, Corrective Action Request, and Opening and Closing Meeting Attendance forms when completed must be sent to the President for review. The President will review the records and determine whether recertification of the Client is justified, unless the President is a member of the audit team. Records of all recertification audit activities are maintained in accordance with the GMCS Control of Records Procedure.

GMCS clients are required to develop and present a presentation demonstrating how their organization has evidenced continual improvement as it relates to management system standards during the previous three (3) year period.

If GMCS has not completed the recertification audit or if GMCS is unable to verify the implementation of corrections and corrective actions for any major nonconformity prior to the expiry date of the certification, then recertification shall not be recommended, and the validity of the certification shall not be extended. The client shall be informed, and the consequences shall be explained.

Following expiration of certification, the certification body can restore certification within 6 months provided that the outstanding recertification activities are completed, otherwise at least a stage 2 shall be conducted. The effective date on the certificate shall be on or after the recertification decision and the expiry date shall be based on prior certification cycle.

1200 G Street, NW, Suite 800
Washington, DC 20005
(202) 351-6837

When a management system standard change (e.g. ISO 9001:2008 to ISO 9001:2015), the client must provide evidence that internal audits have been conducted against all of the requirements in the new version of the management system standard (unless excluded with justification, all organizational processes, and at all sites (i.e. multi-site organizations). The failure of the client to provide clear evidence of these internal audits as stated in form of audit checklists, audit plans and schedules, and audit reports will be cited as a systemic nonconformance and will prohibit a recommendation for recertification or certification until such evidence is provided. In addition, at least one (1) Management Review meeting must be conducted, and any and all affected documents must be reviewed and must conform to the requirements of the new version of the management system standard.

R. Multi-Site Audits Using Sampling-GMCS maintains a procedure on multi-site auditing (GMCS Procedure for Multi-Site Auditing GMCS-MSA-01).

GMCS will appoint a Lead Auditor for any multi-site audit. The Lead Auditor will appoint additional auditors, as necessary, to conduct audits at selected sites within the multi-site sampling plan.

All Multi-Site Audits Using Sampling require the use of the Audit Plan (GMCS-AP-01), Opening Meeting Agenda (GMCS-OMA-01), Closing Meeting Agenda (GMCS-CMA-01), Opening and Closing Meeting Attendance Record (GMCS-AAR-01), Corrective Action Request (GMCS-CAR-01), if applicable, and Audit Report. The Audit Plan, Audit Report, Corrective Action Request, and Opening and Closing Meeting Attendance forms when completed must be sent to the President for review. These forms should be used for each site audited. In the case of the Checklist, there should be one Checklist completed by each auditor for each site the auditor assesses.

All audit records are sent to the GMCS Certification Committee who is responsible for following GMCS Certification Committee Rules and Guidelines GMCS CCRG-01. In the event that one site fails to meet the requirements of the management system standard and/or the Client's management system (defined as one or more major nonconformances), the Client will not be granted certification until the major nonconformance is effectively corrected and verified by GMCS.

The GMCS Certificate of Conformance shall list the sub scopes for each site as stated in the Client's documented scope of its Management System and as verified by GMCS. Temporary sites shall be identified as temporary on the Certificate.

1200 G Street, NW, Suite 800
Washington, DC 20005
(202) 351-6837

S. Multi-Site Audits without Sampling-For GMCS Client's with multiple sites who do not want or that are not eligible for sampling, this Audit Procedure (APR-01) shall govern all aspects of the Audit Process.

The GMCS Certificate of Conformance shall list the sub scopes for each site as stated in the Client's documented scope of its Management System and as verified by GMCS. Temporary sites shall be identified as temporary on the Certificate.

T. Adding Additional Sites and/or Processes to An Existing Certificate of Conformance-Clients may request that additional sites and/or processes be added to their existing Certificate of Conformance. In these cases, GMCS will review and evaluate the request to determine the need for one of the following: 1) grant the extension only after a special or surveillance audit has been conducted, OR 2) issue a revised Certificate of Conformance and review the additional sites and/or processes at the next scheduled audit.

When an audit is conducted, all of the requirements governing GMCS audits, with the exception of the Certification Committee, will apply and all required records, including specific records evidencing that the additional sites and/or processes were audited will be maintained. In the event that the President is a member of the audit team, the GMCS Certification Committee shall be convened and a record of their decisions shall be maintained.

U. Short-Notice Audits-GMCS may find it necessary to conduct audits of certified clients on short notice to investigate GMCS client complaints or in response to changes or as follow-up on suspended clients. GMCS has not accounted for these short-notice audits in its Certification Agreement and/or other contractual documents (e.g. a Technical Proposal submitted to a government client) and the client will need to provide funding and required procurement documents to ensure that these required audits occur. All audit records described in this Procedure must be evidenced as part of any short-notice audit.

For ISO 13485 clients, Short notice or unannounced audits may be required when: a) external factors apply such as: i) devices in scope of certification indicate a possible significant deficiency in the quality management system, ii) significant safety and performance related information becoming known to the CAB b) significant changes occur which have been submitted as required by the regulations or become known to the CAB, and which could affect the decision on the client's state of compliance with the

1200 G Street, NW, Suite 800
Washington, DC 20005
(202) 351-6837

regulatory requirements c) when required by legal requirements under public law or by the relevant Regulatory Authority.

The following are examples of such changes which could be significant and relevant to the CAB when considering that a short notice or unannounced audit is required, although none of these changes should automatically trigger a short term or unannounced audit: a) QMS – impact and changes: i) new ownership ii) extension to manufacturing and/or design control iii) new facility, site change a. modification of the site operation involved in the manufacturing activity (e.g., relocation of the manufacturing operation to a new site or centralizing the design and/or development functions for several manufacturing sites) iv) new processes, process changes a. significant modifications to special processes (e.g., change in production from sterilization through a supplier to an on-site facility or a change in the method of sterilization) v) QM management, personnel a. modifications to the defined authority of the management representative that impact: i. quality management system effectiveness or regulatory compliance ii. the capability and authority to assure that only safe and effective medical devices are released b) product related changes: i) new products, categories ii) addition of a new device category to the manufacturing scope within the quality management system (e.g., addition of sterile single use dialysis sets to an existing scope limited to haemodialysis equipment, or the addition of magnetic resonance imaging to an existing scope limited to ultrasound equipment) c) QMS & Product related changes: i) changes in standards, regulations ii) post market surveillance, vigilance An unannounced or short-notice audit may also be necessary if the CAB has justifiable concerns about implementation of corrective actions or compliance with standard and regulatory requirements (see IAF MD 9, Section 9.6.4.2).

V. Nonconformances-All nonconformances discovered during any type of GMCS must be classified by the GMCS auditor. This classification is subject to review and possible correction by the GMCS Certification Committee. The classification system used by GMCS is as follows and is consistent with the definitions contained in ISO 17021-1:

Major-defined as a systemic, wide-spread failure to meet requirements, multiple minor nonconformances affecting the same requirement, and/or repeat nonconformances (regardless of whether the previous nonconformance was MAJOR or MINOR).

Minor-defined as a non-systemic failure to meet requirements or a lapse in the management system.

GMCS requires Clients to provide a corrective action plan within 30 calendar days of receiving a MAJOR nonconformance. A follow-up audit must occur within six (6) months

1200 G Street, NW, Suite 800
Washington, DC 20005
(202) 351-6837

to ensure that the plan was effectively corrected, unless the Client's Certificate of Conformance expires sooner than six (6) months, in which case, the follow-up audit must occur within thirty (30) days of the Certificate expiration to ensure no lapse in Certification. This audit may be conducted on or off site depending upon the nature of the nonconformance. If the Client fails to provide the plan, effectively implement it, and/or allow the follow-up audit to occur, certification will be denied (for new clients) or certification will be suspended (for existing clients). The costs associated with this verification are NOT included in the estimate or price proposal provided by GMCS to the client. The client must ensure that there is funding and the necessary procurement document in place to ensure that these required audits occur.

It is a requirement that the actions associated with any MAJOR nonconformance be independently reviewed by a member of our Certification Committee. No auditor on the audit team which discovered the MAJOR nonconformance may serve in this capacity. The purpose of this review is to determine whether the client's certification can be maintained.

Clients receiving Minor nonconformances must submit a Corrective Action Plan within thirty (30) calendar days of receiving the Minor nonconformance. Verification that the Corrective Action Plan was effectively implemented will occur during the next scheduled audit. Clients who fail to respond to respond with an effective plan within this timeframe will not be granted certification (new clients) or will have their Certificate of Conformance suspended (existing clients).

Observations and Opportunities for Improvement should be documented in the Audit Report. However, the client is not generally required to respond to Observations and Opportunities for Improvement, unless the Audit Report clearly states otherwise.

Note: The client is responsible for notifying the Lead Auditor of any existing corrective action which has already been recorded to address a nonconformance discovered by a GMCS Auditor. Provided that the client's corrective action as recorded deals directly with the nonconformance discovered by a GMCS Auditor, GMCS shall document the nonconformance as an Observation with reference to the client's corrective action number.

W. <u>Corrective Action Requirements</u>

1200 G Street, NW, Suite 800
Washington, DC 20005
(202) 351-6837

GMCS clients are required to use the GMCS Corrective Action Form CLCAR-01. Clients are provided with this Form for each nonconformance cited during an audit prior to the Closing Meeting.

Using the GMCS CAR Form, the client is required to submit a root cause analysis and corrective action plan in accordance with the Form CLCAR-01 instructions within 30 calendar days of the audit ending. The client submits each CAR Form to the GMCS Lead Auditor.

The GMCS Lead Auditor is responsible for reviewing the adequacy of the root cause analysis and corrective action plan and reasonableness of the stated deadline. The Lead Auditor will either accept or reject the Plan based upon the information submitted by the Client. If the CAR is rejected, it must be resubmitted for review within 30 calendar days. *Note to GMCS Clients, do not use the same deadline for all CARs. Each nonconformance has a separate order of magnitude of effort to resolve the nonconformance which will result in different deadlines for different corrective actions.*

Short-term corrective action will be verified by a GMCS Lead Auditor during the next audit after the deadline stated on the CAR Form. GMCS auditors should not review any CAR during an audit which is not yet due. Prior to GMCS verifying short-term corrective action, the Client must conduct an internal audit of the corrective action implemented to verify that it was done and that it was effective. The Client internal audit must be conducted no later than the implementation due date identified in the client's corrective action plan. If this internal audit does not occur as required, the GMCS auditor(s) shall not review the correction action plan implementation AND shall document a nonconformance for the client's failure to conduct such an audit. In addition, the CAR(s) which could not be reviewed shall be documented in the Audit Report. These unreviewed CARs may be subject to a Special Audit. Audit records of these activities must be maintained and presented to GMCS and shall include checklists and audit reports. The client auditor(s) conducting this audit must be independent from the person proposing and implementing the corrective action. If a Client implements the corrective action plan prior to the deadline BUT fails to conduct the internal audit required, the GMCS auditor is instructed to document this issue as a nonconformance and instruct the client to resubmit the CAR with a new deadline within 30 calendar days of the audit ending. The audit report should reflect this information.

All GMCS clients must submit a request in writing if a root cause analysis, corrective action plan, and/or deadline for implementation requires change or modification. Such a request MUST OCCUR PRIOR to the existing deadline stated on the accepted

1200 G Street, NW, Suite 800
Washington, DC 20005
(202) 351-6837

CAR Form. GMCS Auditors are instructed to document a nonconformance for any GMCS CAR that has not been fully implemented including the internal audit by the stated due date. In addition, GMCS auditors must instruct the Client to revise the corrective action plan and/or deadline within 30 days of the audit being completed and submit it to the Lead Auditor for approval. The audit report should reflect this information. Clients are cautioned not to make changes or extend deadlines until they receive concurrence and approval in writing from GMCS.

X. **Upgrading to Revised Standards**

Clients requesting an upgrade to a new revision of a standard (e.g. ISO 9001:2015, ISO 14001:2015, etc.) may request that the upgrade occur during a special audit, a surveillance audit, or during a recertification audit. A Stage 1 and Stage 2 audit is not required for an upgrade to a new version of a standard, unless the client's certificate has expired, has been revoked, or there is reason to believe that systemic failure of the management system has occurred.

Y. **Special Requirements for ISO 13485, ISO 45001, and ISO/IEC 27001 Clients**

1. **For all ISO 13485 clients**, Client acknowledges and agrees that audit reports and corrective actions shall be submitted to governmental regulators upon request (see IAF MD 9, Section 5.1).

2. **For ISO 45001 clients**, the Client acknowledges and agrees that it shall inform the GMCS, without delay, of the occurrence of a serious safety incident or breach of a safety regulation necessitating the involvement of the competent regulatory authority (see IAF MD 22).

3. **For ISO/IEC 27001 clients**, prior to any audit, GMCS shall ask the client to report if any ISMS related information (such as ISMS records or information about design and effectiveness of controls) cannot be made available for review by the audit team because it contains confidential or sensitive information. GMCS shall determine whether the ISMS can be adequately audited in the absence of such information. If GMCS concludes that it is not possible to adequately audit the ISMS without reviewing the identified confidential or sensitive information, it shall advise the

1200 G Street, NW, Suite 800
Washington, DC 20005
(202) 351-6837

Client that the audit cannot take place until appropriate access arrangements are granted.

In addition, the Client shall ensure that the Statement of Applicability when revised by the Client is sent to GMCS at the time the revision is made. Failure to send GMCS a revised Statement of Applicability shall result in a documented nonconformance.

Z. Climate Change: Effective February 22, 2024, ISO has amended (not revised) the following standards to include a requirement that climate change be explicitly considered as an internal/external issue. GMCS is required to assess this requirement immediately. It is expected that clients have evidence of this consideration in documentation including management review, identified risks, and identified internal/external issues.

ISO 9001:2015, ISO 14001:2015, ISO 45001:2018, ISO 22000:2018, ISO 39001:2012, ISO 37101:2016, ISO 41001:2018, ISO 37001:2016, ISO 21001:2018, ISO/IEC 20000-1:2018, ISO 50001:2018, ISO/IEC 27001:2022, ISO 37301:2021, ISO 22301:2019

AA. **Notification to GMCS by Client**-The Client is responsible for notifying GMCS in writing (LBRAND@GMCS.US) of the following changes to its Management System in real-time: 1) The documented scope of the Management System has changed, 2) The organization has undergone significant management changes, 3) There have been significant changes to the organization's work site(s) (including adding or removal of shift work), 4) The organization's management system has undergone significant change(s).

AB. **Remote Audits-**To be eligible for a remote audit, the client must be in a service (i.e., non-manufacturing/production environment) where the difference between an onsite audit and a remote audit is negligible. In addition, the client must have the technology to facilitate a remote audit (e.g., MS Teams, Google Meets, etc.) which is compatible with and accessible by GMCS and its personnel.

The GMCS Audit Plan and Audit Report contain specific information on whether remote auditing is used, the technology utilized to facilitate the audit, and any issues discovered during a remote audit which are specific to the use of remote auditing.

1200 G Street, NW, Suite 800
Washington, DC 20005
(202) 351-6837

For ISO/IEC 27001 clients, the following additional factors stated in ISO/IEC 27006-1 shall apply:

a) available infrastructure of the certification body and the client;

b) sector in which the client operates;

c) type(s) of audit during the certification cycle from initial audit to recertification audit;

d) competence of the persons of the certification body and the client, who are involved in the remote audit;

e) previously demonstrated performance of remote audits for the client;

f) scope of the certification.

The analysis shall be performed prior to performing any remote audit. The analysis and the justification for use of remote audit during the certification cycle shall be documented.

The audit plan and audit report shall include clear indications if remote audit activities have been performed.

Remote audits shall not be used if the risk assessment identifies unacceptable risks to the effectiveness of the audit process.

The risk assessment shall be reviewed during the certification cycle to ensure its continued suitability.

NOTE In case the client uses virtual sites (i.e. location where an organization performs work or provides a service using an online environment allowing persons involved to execute processes irrespective of physical locations), remote audit techniques are a relevant part of the audit plan.

1200 G Street, NW, Suite 800
Washington, DC 20005
(202) 351-6837