Level III Inspection

1. **Purpose / Background**
   EHS – MS Inspections serve to promote, monitor and focus on compliance with regulations and best practices that apply to research and operations at MIT. Three tiers of inspections within this program have been established.

   Level I Inspections are conducted at the local level and focus on routine activities such as managing hazardous waste.

   Level II inspections are conducted at the wider DLC level and are performed by a team established by the DLC-EHS Coordinator and EHS Lead Contact. The team employs a formal inspection process to identify record and report activities/conditions which require correction. All level II inspection results are maintained in a central database.

   Level III audits are conducted by an approved third party group with a goal to evaluate the overall effectiveness and sustainability of the EHS Management System (EHS-MS). Audits may include compliance or system audits as determined by the EHS Office, MIT Audit Division and Institute Council on EHS. Level III audit criteria and results are maintained by MIT Audit Division and/or the EHS Office.

2. **Scope**
   This procedure applies to all Research and Operations divisions at MIT and its satellite locations.

3. **Prerequisites**
   Level III Audits are conducted within the criteria established within this SOP.

4. **Procedures**
   4.1 **Frequency**
   Level III audits are performed at least every two years by an approved third party auditor. This may include entities contracted by the Institute and approved by the Audit division or by MIT Audit Division approved by EHS Management.

   4.2 **Inspection Team**
   Level III audits are performed by the MIT Audit Division (MIT Audit) or an outside entity. EHS Management (Director and Managing Director) and MIT Audit will review and approve the qualifications, as appropriate; of auditors whenever a third party external to MIT conducts a Level III audit.

   4.3 **Audit Planning**
   Audit planning includes: scope and objective(s), protocol, team composition/leadership, entrance meeting, documents required for the review, timeline, data management, contact people, audit program and reporting structure.
When a Level III audit for a given area within the EHS-MS is performed by an outside entity, EHS informs MIT Audit. Audit reviews the scope and the objectives of the review to ensure that it is within the requirements of this third tier type of EHS review.

When the review is performed by MIT Audit, the process starts with the selection of a component(s) within the EHS-MS to be targeted for this assessment. The selection is made independently by the auditors while consulting with EHS for current higher exposure areas, or other areas of interest.

The planned review along with its scope and objectives is presented to Institute Council on EHS.

4.4 Conducting the review

When review is performed by an outside entity, MIT Audit ensures the review is completed independently and that scope and objectives are clearly defined. MIT Audit also monitors the progress and participates in final meetings to discuss the results.

When a review is performed internally, Audit defines the objectives and the scope of the review and proceeds to determine business objectives, risks and controls of the related component or process reviewed. Under guidance established by the MIT Audit Committee, MIT Audit strives to perform their work in accordance with the *International Standards for the Professional Practice of Internal Auditing* issued by the Institute of Internal Auditors. Reference to this organization is provided later in this report.

Processes reviewed are documented and a risk/exposure analysis is performed to prioritize audit testing and perform selected tests of those controls. This determination is essential for providing reasonable assurance that internal audit resources are deployed in an optimal manner.

In the setting of objectives and scope for a review, Audit relies on the adequacy of general computer controls which are generally excluded from the scope of individual process audits. Application controls, when not covered elsewhere, are likely to be considered within the scope of the audit.

4.5 Documenting Findings

Each finding/observation is documented and supported by pertinent information relating to the audit issue. Finding detail may include a missing control, a breakdown in control, or any related inefficiencies.

For reviews performed by outside entities, MIT Audit reviews the findings, recommendations. EHS responses and provides additional clarification and/or recommendations as necessary.

4.6 Reporting

For reviews performed by MIT Audit, findings are documented in a draft audit report and exit meeting notes which are discussed with EHS at a formal exit meeting. Audit issues a final report to EHS Management including management responses and action plan. Audit reports are made available for Audit Committee review.

For external audits, MIT Audit reviews the initial draft report and consults with EHS Management on adequacy of responses.

An official hardcopy of this document exists in the EHS Office or on the EHS website. See Legal Disclaimer at: [http://ehs.mit.edu/site/content/legal-disclaimer](http://ehs.mit.edu/site/content/legal-disclaimer)
Summary of the audit findings are included in the annual Environmental Programs/EHS Headquarters (EP/EHO) and EHS Office report to the President and are also distributed to the Institute Council on EHS. Follow up process

Findings are rated high, medium or low relative to potential risk. High and medium rated findings are reported and tracked in greater detail during a formal follow-up process. Audit completes the follow up for reviews performed both internally and by external entities.

5. Roles & Responsibilities
EHS Management and MIT Audit is responsible for managing the Level III process which includes: audit planning, identification of proposed audit focus, selecting an audit team, developing scope and objectives, submitting audit plan for approval, conducting the audit, reporting results and coordinating follow-up.

6. Training
All individuals responsible for participating in a Level III audit must have appropriate training and experience as determined by EHS and MIT Audit Division Management.

7. Monitoring Requirements
The MIT Audit Division monitors outside entities performing Level III reviews to ensure they are completing the work in an independent manner, that they have adequate procedures and have defined their objective and scope of the review.

8. Record Management
The results of all Level III Audits are maintained at EHS Management Office and MIT Audit Division.

All MIT Audit Division review related data is stored in an integrated software package that is comprised of several modules:

- Planning of Audit: the system allows risks and controls to be assessed and assurance work to be planned and carried out;
- Working Papers are stored as attachments;
- Draft and Final audit reports can be automatically produced;
- Follow up documentation - actions are documented based on client’s responses and can be tracked through the system.

For external review, findings, recommendations, responses and follow up status are also documented by Audit in the above mentioned software package.

9. References
MIT Audit Division Standards and Policies

10. Definitions
- Audit: According to the International Standards for the Professional Practice of Internal Auditing, internal auditing is an independent, objective assurance and
consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

- **Third Party:** A third party refers to an individual or group of individuals who function independently from the process and oversight of EHS and are recognized for their competency in judgment and evaluation of the audit requirements.

- **Findings:** Significant observations that could adversely impact the organization.

- **Audit Report:** Includes details related to findings that could negatively impact the organization and whether or not they have been satisfactorily resolved or have an action plan in place. Audit reports may also include potential improvements to those processes reviewed during an audit.

- **Audit Test:** Audit test includes inquiry of business unit personnel, inspection of documents and records indicating performance of the control, observation of the application or existence of specific controls and re-performance of the control to test the accuracy of its operation.

- **Audit Objective:** Audit review objectives encompass gaining an understanding of a business process and evaluating the adequacy and effectiveness of related controls.

- **Scope:** Scope represents the degree of testing required to achieve the audit objectives in each phase of the engagement. Scope statements will usually include the engagement period, objectives, risks, processes and transactions that should be included in the audit work.

- **Work Papers:** Work papers represent a permanent documentation of what occurred during the course of an audit. They should record information obtained and analysis made as well as support the basis for the findings and recommendations in the audit report.

- **Entrance Meeting:** Initial meeting with business process owner and/or stakeholder(s) to introduce audit team, present audit process (from selection of engagements through follow-up), present audit objectives and scope, confirm contact person(s) and schedule, request relevant documents, and solicit business process owner and/or stakeholder input on risks and other requests.

- **Exit Meeting:** Meeting with business process owner and/or stakeholder(s) to discuss preliminary findings (condition; criteria; effect; cause; recommendation).

- **Audit Follow up:** Follow up work is performed to ensure that management's corrective actions have been put in place and are adequate to alleviate the findings noted within our report. Follow up is performed on corrective actions, not audit recommendations.

- **General Controls:** General IT controls are controls over the IT environment, including organizational and administrative activities, infrastructure and environmental controls over how systems are linked, and physical security over IT assets and physical and logical access.
• **Application Controls:** Application controls are more specific than general IT controls in that they only address the application under review. Application controls dictate how the application processes information and passes it to subsequent applications and govern role-based security.

• **Business Objectives:** Business objectives represent goals of the business unit (i.e., things that are important to the process owners). All business objectives should be validated with the business process owner.

• **Risks:** Risks are threats, failures, errors or other items that may interfere with attaining the business objective.

• **Controls:** Controls represent activities, including established policies and procedures, to ensure that management’s directives are implemented and applicable risks are managed.

• **Who is IIA:** The Institute of Internal Auditors is the internationally recognized standard- and guidance-setting body for the internal audit profession globally and promotes guidance following rigorous due process. By providing authoritative guidance, The IIA sets the bar for internal audit efficiency, effectiveness, and professionalism.

• **International Professional Practices Framework (IPPF):** The conceptual framework that organizes authoritative guidance promulgated by The Institute of Internal Auditors that delineates the requirements for performing a broad range of audit activities and for evaluating internal audit performance.

• **The MIT Audit Division** delivers audit services through a risk-based program of audit coverage featuring business process reviews, targeted reviews, capital construction cost reviews, site visits, departmental assessments and advisory services to provide assurance to management and the Audit Committee that good business practices are adhered to, adequate internal controls are maintained, and assets are properly safeguarded. Audit Division conducts the work through these various engagement types that are designed to provide value to the Institute based upon the maturity of the business process, the implied or inherent risk profile of the area, and the most effective approach to achieve the objectives of the review.

While reporting administratively to the Executive Vice President and Treasurer, the Audit Division is fully attentive to the support and service of its primary customer, the Audit Committee of the Corporation. The MIT Audit Committee meets three times per year, in accordance with its charter that lends momentum to the Audit Division’s goals for monitoring internal controls and supporting the Institute’s risk management processes.