



# IOCE Laboratory Management

## Contents

Customer Identification

Investigator v. Technical Support

Organization: Service Delivery Models: Independence and Objectivity

Outsourcing

Facility Design

Equipment Modules

Training

Personnel: Selection – Burnout – Stress

Performance Measures

Quality Assurance: Performance Testing: Accreditation: Validation

Archives: Data Retention Policies

Examination Tools

Health and Safety

Secure Executive Level Support

Procurement Philosophy/Strategy

Evidence Handling

**1. Customer Identification:**

Needs to be updated on a regular basis.

Agents/Investigators are principal customers.

Mission creep can undermine your main mission. Everyone wants support.

Need to have priority system for cases, e.g. murder, internal affairs, due in court, etc.

Priority system is lab specific issue.

Customer base may include investigators as well as Internal Affairs and others.

**2. Investigator v. Technical Support:**

Emphasis should be on the quality (competency) of examination personnel.

Closer scrutiny of functions needs to be considered:

- Who does collection of evidence;
- Who gathers basic investigation facts (subscriber checks);
- Who performs detailed examinations.

Accreditation standards will apply for anyone doing examination work.

Management should insure the examiner is neutral.

Argument for sworn investigator/examiner personnel is ability to retain them.

Ideal is to separate the investigative role from the forensic/evidence role.

Technical sophistication in computer systems is creating strong need for very specialized/trained personnel or “teams” of examiners to perform the exams.

**3. Organization: Service Delivery Models: Independence and Objectivity:**

Most organizations use either a central or distributed model.

Service model should fit your agency's operational need. Determining factors can be geographic area of coverage, national laws, and agency size.

Decentralized organizational structures require strong central program management.

Service model needs to reflect case workload, case priorities, and operational economics.

Legal system, search warrant rules, and scope of warrant are the most significant determining factors on how service delivery models are designed.

**4. Outsourcing:**

Two forms of outsourcing:

- On-site (at the forensics lab) examiner support
- Sending evidence to outside businesses.

Outsourcing must maintain chain of custody and be performed in accordance with forensic science principles, current best practices, and comply with the organization's quality standards.

Outsourcing can provide scarce technical expertise, or supplemental manpower support.

Outsourcing is used as supplemental staffing strategy at several computer forensic laboratories.

**5. Facility Design:**

Facility proposals should be comprehensive and have growth options. A good business plan is essential to securing recurring and expansion funding.

Good facility design enhances evidence control and minimizes evidence cross contamination.

Good facility design should take into consideration employee health and safety and the local building code.

Laboratories must have an access control system.

Lighting, AC power supplies, ground fault circuits, and uninterruptible power supplies are key issues for computer forensic laboratory design.

**6. Equipment Modules:**

Equipment modules are a standardized set of equipment and software that is assigned to individual or groups of examiners.

Equipment modules are good budget techniques to secure financial resources. Both individual and laboratory or group modules are used.

Equipment modules promote hardware and software standardization.

Equipment modules are an effective means to schedule replacement lifecycles.

Equipment modules may simplify equipment and software validation.

Equipment modules are useful in medium to large-scale organizations.

**7. Training:**

Good leverage technique is to use academia, private industry or software vendors.

In-house R & D is an effective means to have advanced training.

Trainers need to communicate better so that curriculums are not re-invented. Training methodologies and simulated cases (or exercises) should be shared at the international level. This is a matter of efficiency and duplication avoidance.

Independent training sources are very basic. In-house training is used at all laboratories and seems to be fairly effective.

Core training requirements need to be identified in US. Australia has a central program consisting of curriculums and qualification tests.

Law Enforcement needs to articulate more detailed requirements (network forensics, volatile memory forensics, etc.).

Training needs to be linked to laboratory accreditation and individual examiner certification.

**8. Personnel: Selection – Burnout - Stress:**

Start up work is substantial – position descriptions and recruitment.

Key qualities to look for: investigator's attitude, interest in computer forensics, some previous IT training.

Different backgrounds have advantages and disadvantages. General recruitment categories are: Law enforcement professionals, IT trained individuals, compute/cyber crime trained individuals, self-taught individuals, and civil litigation/search personnel.

Interview process needs to identify personnel that have basic skills and problem solving techniques.

Skill demonstration may be a valid interview technique.

Child pornography investigations can cause examiner burnout, latent stress. Rotational assignments and professional monitoring are recommended.

Examination backlogs and never ending case support requests cause stress and forced annual leave can be in the best interest of the employee if allowable.

Managers must observe and recognize burnout in employees and use training, conferences, meetings, and professional development to help pace employees.

**9. Performance Measures:**

Experience levels do affect productivity.

Hard drives and volatile memory objects are counted and individual examiners compared to the mean.

Qualitative factors (training, collateral administrative duties) need to be considered in evaluations.

Senior examiner performs a triage assessment and the actual examiner's time expenditure is compared to the expected.

A degree of difficulty system without triage is not recommended.

Case type (fraud, drug, murder) does affect average processing time.

Pass/Fail or rating on organizational values should also be included.

Clear work plans are a fair way of setting objectives.

Management information and accounting systems are recommended to track performance.

Measurement items are: hard drives, CDs, diskettes, gigabytes, volatile memory objects, cases.

**10. Quality Assurance: Performance Testing: Accreditation: Validation:**

Need to identify a quality manager.

Proficiency testing is essential to quality control.

Most laboratories are not doing proficiency tests at present, but its need/importance is recognized.

Sharing of tests among agencies is considered an efficient test technique.

ISO quality assurance concept focus is on end result.

It is important to know and test your standard operating process.

Results should be repeatable and valid.

Quality Assurance must be consistent with accrediting body's standards (ISO, ASCLD/Lab).

**11. Archives: Data Retention Policies:**

Original evidence is always returned.

Duplicate evidence is sometimes archived 5-10 years while other organizations return the duplicate with the original evidence.

Legal rules for each jurisdiction dictate what data retention policies are appropriate.

**12. Examination Tools:**

Management must control tools used in the laboratory.

Issues are tool validity and tool license.

**13. Health and Safety:**

Concerns are: biological or chemical evidence contamination. Laboratory equipment/structures need to be ergonomically designed.

All applicable health and safety rules and regulations need to be followed.

Additional safety protocol may include cell phones and or requiring two or more employees to be present when examining evidence.

**14. Secure Executive Level Support:**

Keep dialogue open with top management.

Develop business plan (startup & recurring).

Institute charge back system for large or unusual equipment or software costs.

Present war story cases to keep executive level interest.

Use graphs and numbers to make points in executive briefings.

Use agency analogy examples to justify the direction to go in.

**15. Procurement Philosophy/Strategy:**

Life cycle for computer forensic hardware is around 3 years and 12 months for software is recommended.

Authority for emergency procurements (hardware or software) needs to be available for case support.

Organizational structure can be a major factor in justifying sole source procurements to maintain compatibility.

Decision maker authority to approve procurement should be in the lab.

**16. Evidence Handling:**

Group considers that leaving digital evidence out in the lab to duplicate, keyword search work copies and password crack files is acceptable as long as the laboratory meets agency evidence storage standards.

Evidence information systems are desirable to track evidence location, receipt and release.