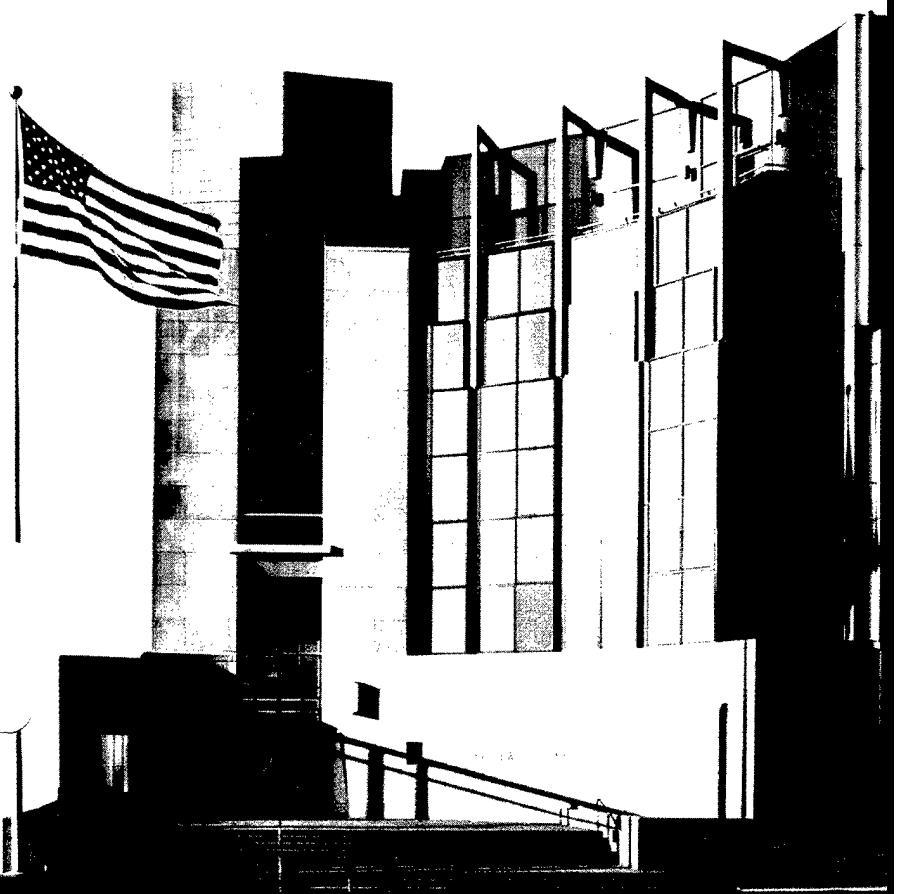
Carnegie Mellon
Software Engineering Institute

Case Study: Computer Supplier Evaluation Practices of the Parenteral Drug Association (PDA)

David Carney
Harvey Greenawalt
George Grigonis
Patricia Oberndorf

May 2003



TECHNICAL REPORT
CMU/SEI-2003-TR-011
ESC-TR-2003-011

Carnegie Mellon
Software Engineering Institute

Pittsburgh, PA 15213-3890

Case Study: Computer Supplier Evaluation Practices of the Parenteral Drug Association (PDA)

CMU/SEI-2003-TR-011
ESC-TR-2003-011

David Carney
Harvey Greenawalt
George Grigonis
Patricia Oberndorf

May 2003

COTS-Based Systems Initiative

This report was prepared for the

SEI Joint Program Office
HQ ESC/DIB
5 Eglin Street
Hanscom AFB, MA 01731-2116

The ideas and findings in this report should not be construed as an official DoD position. It is published in the interest of scientific and technical information exchange.

FOR THE COMMANDER

Christos Scondras
Chief of Programs, XPK

This work is sponsored by the U.S. Department of Defense. The Software Engineering Institute is a federally funded research and development center sponsored by the U.S. Department of Defense.

This work was created in the performance of Federal Government Contract Number F19628-00-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

For information about purchasing paper copies of SEI reports, please visit the publications portion of our Web site (http://www.sei.cmu.edu/publications/pubweb.html).

Table of Contents

List of Figures

List of Tables

Abstract

This case study describes the development of a method for evaluating computer and software suppliers for the pharmaceutical industry. The study describes the role of government regulation within the industry and the need for standardized audits of computer and software suppliers.

The audit method consists of six steps: initiation, pre-work, auditing, observations and reporting, decision, and follow-up. Each of these steps is described in detail, as are several features of the method: a data collection tool, an audit repository, and extensive auditor training supervised by an industry-regulated oversight agency.

Finally, the report describes the benefits of this audit method, together with a set of lessons learned about the audit of computer and software suppliers.

1 Background

The Parenteral[1] Drug Association (PDA) was founded in 1946 by a group of pharmaceutical manufacturers who recognized the need for an organization to disseminate information within the pharmaceutical industry. Today PDA is a non-profit international association of scientists involved in the development, manufacture, quality control, and regulation of pharmaceuticals and related products. The association is coordinated through its headquarters in Bethesda, Md. and a Training and Research Institute outside Baltimore, Md. The mission of PDA is to support the advancement of pharmaceutical technology by promoting scientifically sound and practical information and education for industry and regulatory agencies.

The Software Engineering Institute (SEI[SM]) is a federally-funded research and development center located at Carnegie Mellon University, Pittsburgh, Pa. The U.S. Department of Defense established the SEI to advance the practice of software engineering since software represents a growing element of U.S. defense systems. The SEI mission is to provide leadership in advancing the state of the practice of software engineering in order to improve the quality of systems that depend on software. Practices and techniques for software evaluation, particularly of commercial off-the-shelf (COTS) software, are of interest to the SEI.

PDA and the SEI met early in 2000 to discuss PDA's work with COTS software. PDA had developed a standardized process model for auditing and evaluating computer suppliers and vendors. Both organizations agreed to describe the PDA process model and its use in a case study, to be published as one of a series of SEI case studies detailing various aspects of COTS software. This document is the result of that joint effort.

1.1 Audits of PDA Suppliers

Computers and computer software now play a critical role in the pharmaceutical industry. Computers are involved in the discovery, manufacture, and delivery of drug products, as well as in the engineering, manufacture, and delivery of medical devices. The pharmaceutical industry is heavily regulated by the Food and Drug Administration (FDA) and, in the case of

---

1 *Parenteral* is defined as "taken into the body or administered in a manner other than through the digestive tract" (American Heritage Dictionary). This term refers to pharmaceutical medicines and technologies.

SM SEI is a service mark of Carnegie Mellon University.

computer technology, each pharmaceutical firm is accountable for correct and reliable computer systems. There is thus a need to assure the quality of the industry's computing environments and for validation of each firm's computer systems. Making this especially challenging is that pharmaceutical companies are increasingly dependent on external suppliers for their computer systems, both hardware and software.

At the start of the 1990s, audits to support validation of computer-related systems began to become commonplace within the pharmaceutical industry. These audits have grown in frequency, and the entire pharmaceutical community has experienced dramatic increases in the number of audits being conducted. During the ensuing decade, the industry also witnessed a significant increase of new suppliers being audited, largely due to increased use of emerging computer technologies by pharmaceutical companies. Many of these new suppliers had never previously experienced audits motivated by regulatory compliance expectations.

Originally these audits were executed primarily by compliance personnel in pharmaceutical companies who possessed a basic knowledge of software processes; they used methods and checklists common to auditing physical processes and checking paper trails. Much of this behavior was based on written regulations for good manufacturing and good clinical practices, but it was hardly suited for technology processes.

The burden of external auditing was becoming costly and unmanageable for both the pharmaceutical companies and their suppliers. In 1999, surveyed suppliers reported that

- The length of audits had doubled since 1996, due to more complex software and hardware technologies.
- The average annual cost per supplier to host pharmaceutical company audits was estimated to be $150K - $200K, and at least one supplier reported costs in excess of $200K.
- There was duplication of audits both within and across pharmaceutical companies.
- The competency of auditors had not kept pace with the evolving technology concepts.

Today's audits are more focused on technology processes that produce a software commodity. Personnel involved may still be associated with functional compliance units within the pharmaceutical companies, although this is changing. But they generally possess a greater knowledge of modern technology processes, and are less oriented toward regulatory compliance and more toward the suppliers' compliance with their own internal procedures.

On the customer side (i.e., the pharmaceutical companies), a similar duplication of effort occurred, resulting in inefficient use of limited resources. Diverse auditing methods and inconsistent results produced costly information that had limited utility. At an average cost of $9K per audit, some pharmaceutical companies were spending an estimated $450K per annum in audit execution costs, not including the related costs associated with these audits, for such

things as analyzing outcomes, managing the procured commodity and supplier, and sharing information within the enterprise.

1.2 Need for a Standardized Audit Process

The FDA observed many of these issues firsthand during pharmaceutical company inspections. In 1996, the FDA challenged the industry to establish a standard way to assess supplier organizational practices. The benefit of such a standard would be to support quality judgments by the pharmaceutical companies of the computer products and custom services (e.g., software) they were buying. In addition, the entire industry, including suppliers and regulators, would save money in the process.

As a direct result of that challenge, a supplier auditing and qualification task group was established by PDA. The task group's objectives were to

- define and demonstrate (through simulation and field testing) a process for supplier audits and qualification in a way that promotes standardization and simplification
- meet regulatory expectations for customer due diligence in determining quality of acquired software and computer products in general
- satisfy customer needs for information supporting procurement, systems engineering, and computer validation
- lower audit costs for both pharmaceutical companies and suppliers

The result of the task group's work was a carefully defined process for auditing suppliers of computer products and services to the pharmaceutical industry. The task group also defined a data collection tool, auditor training, repository models, and performance metrics. All of this was documented in a PDA Technical Report [PDA 99].

2 PDA Computer Supplier Audit Process Model

In this section we describe the approach used by the PDA task group to develop the audit process model, and then describe the process model and the testing strategy used to validate it. At the outset, however, we define several key terms that will be used throughout the remainder of this case study.

2.1 Definitions of Key Terms

Client: any person or organization who makes use of the results of the audit process. These are the program subscribers. Clients of audits are typically pharmaceutical companies purchasing computer systems from external suppliers.

Supplier: any person or organization who sells technology products or services in the marketplace and consequently to FDA-regulated clients who purchase from the marketplace. In the typical case, suppliers are the COTS software and hardware providers.

Sponsor: any person or organization who funds the audit of a supplier. The sponsor can be a client or, more often, a department within the client's organization.

Auditor: any qualified person who executes the audit process and is (1) independent from the supplier, (2) not in competition with the supplier, and (3) qualified by PDA to execute the audit process. Auditors are usually persons who are direct employees of the client or sponsor or are members of a qualified third party under contract to the client or sponsor.

Project: any client's computer need being fulfilled through the implementation of COTS products. In a typical case these are information technology projects aimed at a business solution involving computers that are used in regulated activities.

2.2 Development Approach

The task group was composed of representatives from pharmaceutical companies, suppliers, and regulatory and validation services; their work took place over a 27-month period. Among

their initial actions were the creation of a charter and a precise definition of the group's scope. The charter included both an operating plan and a guide to team behavior. The definition of scope was aimed at limiting the work to the execution of audits and documentation of results. Excluded from the scope were such issues as identification of suppliers, allocation of resources, and analysis of audit results.

One major source of information for the task group was the body of existing processes used in other industries for audits. The task group examined the practices of the nuclear, automotive, and defense industries for data on auditing and qualifying suppliers. They also examined in detail the existing practices used within the pharmaceutical industry itself by sampling operating programs in several pharmaceutical companies. The task group collected and analyzed procedures, checklists, templates, and methods used for scheduling, executing and reporting supplier audits.

The examination of industry audit processes revealed a wide array of practice. For instance, the defense industry emphasized methods based on capability determination: defense auditing methods are based on the assumption that past performance is a good measure of future performance. In contrast, the automotive industry relies heavily on the ISO 9000 Quality System Standards. Where these are insufficient, the automotive industry has established additional standards to be used in conjunction with them. In the nuclear industry, power companies evaluate their suppliers using a common method and criteria for assessment; results are shared within the community.

A second major source of information for the task group lay in the needs of the relevant stakeholders of the PDA audit process. There were three communities of stakeholders: pharmaceutical companies, suppliers, and regulators. An initial survey for each of these communities was developed, and the task group analyzed the data from these surveys, together with the results of workshops.

The three surveys revealed different sets of concerns, although there were some common themes among them. For instance, the responses from the pharmaceutical industry indicated that lack of audit standards, need for sharing, and limited resources were the three most significant issues. The regulatory respondents indicated several other issues, but concurred that formal procedures to audit and document supplier capability were an overriding need. The suppliers' major concerns were related to the intrusive element: time and resources needed for audits, and the growing number of audits each year. But the suppliers also expressed frustration relating to variety of audit methods, which is consistent with the other two surveys and the expressed need for audit standards.

Based on both of these sources of data, a process model was gradually developed. The model was revised as more data became available from the ongoing analyses of existing processes

and from the surveys. The result was a draft process model, which is described in the following section.

2.3 Description of the Process Model

The PDA Supplier Audit Process Model incorporates six steps. Each step represents a collection of activities that are shared between pharmaceutical companies, their suppliers, and auditors. The steps are as follows:

1. Initiation: define the scope and objectives of the audit; define the audit team
2. Preparation and Pre-Work: acquire necessary information for planning and scheduling; define and refine criteria; verify team skills
3. Auditing: execute audit per plan
4. Observations and Reporting: document and verify audit results; prepare reports
5. Decision: analyze audit data (analysis by the regulated end user)
6. Follow-Up and Close-Out: terminate audit and prepare for surveillance

To make the execution of audits consistent, the model also includes a set of templates for planning and preparation, establishment of team roles, results reporting, and communication with the supplier to be audited. Execution of this process model is also predicated on several other enabling technologies that are described at length in Section 3. Each audit step is fully documented by PDA [PDA 99]; below we provide a detailed summary of each step.[2].

2.3.1 Initiation

There are two prerequisites for the Initiation step, namely that a supplier has been identified as the target of an audit, and that resources for the audit have been allocated by the audit sponsor. The Initiation step covers the development of the scope of the audit and the selection of the audit team.

An audit may be the initial audit of a supplier, or may occur as part of a monitoring or surveillance activity; monitoring and surveillance will be more fully explained in Section 2.3.6. Scope is principally determined by the client, and includes such details as how the client intends to use a suppliers' product or service; this information is captured in a product profile. An audit's scope also must be defined in the sense that an audit may focus on product documentation, a supplier's service practices, a supplier's technical practices, quality and related

[2] Anyone can contact PDA to get a copy of this report for a minimal cost. Interested parties can see what the program is about, the audit questions, and what is generally needed to implement and use the program.

service, or similar audit areas. Finally, the supplier and the audit team will agree on a schedule for the audit.

The duration of this step is largely dependent on the identification of candidate suppliers whose products will be considered as possible components to the overall computing solution. Risk-based methods and techniques are suitable in determining which candidates are to be subjected to an audit. Completing and validating profiles, identifying target suppliers, and contacting suppliers may take one to five days, depending on task assignments and responsibilities. If qualified third-party auditors are to be contracted, an additional two or three days should be added for analyzing work proposals and issuing contracts for work. Most companies using third-party services for audits have standing professional work agreements in place that facilitate work orders. The ideal team size is one or two auditors; larger teams can cause delays in scheduling and execution.

2.3.2 Preparation and Pre-Work

During this process step, all necessary preconditions for the audit must be met. These include any legal agreements (e.g., non-disclosure documents) between participating parties, regulatory requirements (e.g., Federal regulations), or other standards (e.g., ISO 9001). These preconditions may also include such data as the supplier's organization chart, list of development tools, previous audit reports, and similar information.

After this information has been gathered, a detailed audit plan is prepared. This plan includes

- objectives and scope of the audit
- type of audit (i.e., initial monitoring, surveillance)
- coverage (products that are included)
- identification of the individuals who defined objectives and scope
- identification of all reference documents
- identification of team members
- language of the audit
- date and location of audit
- identification of audit areas to be covered
- planned time and duration of each activity
- expected report distribution

In addition to the audit plan, this step also includes definition of an audit criteria checklist whose elements are distributed among the team members. This checklist is based on a preexisting template that can be modified for a particular audit.

Upon completion of the plan, the supplier is notified and all necessary entrance briefings are schedule. Any disagreements or misunderstandings between supplier and audit team are also resolved at this time.

This step, using either internal resources or a qualified third party, typically takes between one-half and one full day. Since templates for formal communication and data collection are provided, this step rarely takes more than two days. Customer-specific issues may require more preparation time, so it is essential that the audit team understand these issues to ensure timely data collection.

2.3.3 Auditing

The audit is conducted on-site at the supplier's organization. The audit is framed by opening and closing meetings between the supplier and the audit team. At the opening meeting, the supplier is informed of the details of the audit plan, and the details are confirmed and, if necessary, refined (e.g., site tours may be appropriate). At the closing meeting, the preliminary observations are presented by the audit team and acknowledged by the supplier.

The major activity of the audit is examining evidence and collecting data about the supplier's operations and practices. Evidence is collected through interviews with supplier personnel, examination of documents and records, and observation of activities and conditions. The audit criteria checklist helps to document this evidence, ensures that the necessary data is gathered and, along with the audit guide, assists auditors in making observations that are statements of fact supported by objective evidence. The checklist questions are directed at the auditor and not the supplier, thus permitting the auditors to use their own styles and methods to acquire the needed information.

Audits are also expected to be "performance oriented." This means that the audit will stress activities that inspect a supplier's entire operation while emphasizing safety and reliability of the product. The audit team's attention should focus on essential elements of an activity and disregard the inconsequential. To achieve such a focus, vertical slice techniques can be used in conducting audits [ERCI 88].

As the audit is being conducted, daily reviews with all participants (audit team and supplier) are held. Once the team has performed its data-gathering activities, a list of preliminary observations is created, and presented to the supplier during the closing meeting.

The duration of this step is dependent on scope of the audit. Typically software processes and user information require 2 to 2.5 days. Hardware practices and user information require 1 to 1.5 days, as do custom services. Customer-specific requests are variable, but for the most part they have rarely taken longer than half a day.

Note that these audits are process specific and not product specific. Therefore data collection also involves documenting all products affected by the inspected processes, along with artifact sampling to ensure complete coverage of all affected products noted by the auditor. Audits are on everything the supplier does, not just the product of interest to a particular sponsor. If information is needed later on another product, the sponsor can refer to the audit so long as the information is on the list. Otherwise a second audit will have to be conducted.

2.3.4 Observations and Reporting

This step consists of the activities relating to documenting the work of the audit team. The activities for the audit team include preparing the draft of a report, revising and then releasing it, first to the supplier for comment, and then to the PDA Repository (described in Section 3). The supplier's activities include two separate occasions for review, response, and comment on the report.

After all reviews have taken place, the lead auditor places the audit report into the repository, and the report, together with all attendant documents and records, is retained according to the records management practices of the repository.

Explicit durations are defined for all of these activities; such constraints ensure that the results of the audit process will be timely for all parties concerned. For instance, the draft report must be provided to the supplier for comment within 10 working days of the closing meeting; the supplier then has 10 working days to respond in writing with any comments or criticisms of the report. The process provides an additional five working days for resolving and implementing supplier edits to the report.

2.3.5 Decision

As described above in Section 2.2, the task group decided that the analysis of audit results was out of the scope of the process. Therefore, the activities relating to such analysis are defined only generally in the PDA model. Two of these activities are included in this process step: Client Analysis of Supplier Data and Client Supplier Management. Neither of these activities is described in detail, except to indicate that all responsibilities for these activities lie with the clients of the audit.

2.3.6 Follow-Up and Close-Out

The activities performed in this process step all focus on actions taken as a result of nonconformance to expected good practice observed by the audit team.

The supplier is expected to respond to any negative observations, either through correction of some condition or written explanation that would establish equivalency to good practice. The audit team establishes whatever monitoring may be needed and issues periodic reports on the supplier's progress, when there is commitment by the supplier to adjust or improve a practice. Once all the supplier's responses to negative observations have been resolved, the audit is closed. If any issues are still outstanding, a follow-up visit may be performed.

In addition, the PDA model defines a surveillance program to ensure that all supplier information is up-to-date. The model recommends that a maximum surveillance interval of 24 months be chosen. A surveillance audit is necessary at the end of this period or if some other factor (e.g., reported product failure, major organizational change) warrants it.

2.4 Strategy to Test the Model

As the process model was being developed (together with all of the enabling technologies), the task group also implemented a testing strategy consisting of both simulation and field testing. The goal of this testing was to prove the concept and also to confirm alignment with the initial goals of the project.

Simulation testing consisted of executing the model in a hypothetical audit. The participants took the roles of suppliers, auditors, and observers; in the first two cases, the persons were drawn from actual suppliers and pharmaceutical companies. The observers were members of the task group. The result of the simulation testing related mostly to the skills needed by auditors; this data was incorporated into the development of the training materials.

Field testing of the process model took place at three supplier sites in early 1999, when the process model and the enabling technologies were in draft, but were sufficiently stable to be used under actual auditing conditions. The tests did not make use of step six (Follow-Up and Close-Out) but were otherwise full tests of the model, together with its templates and several of its supporting technologies. Suppliers, auditors, and the task group expressed individual assessments of the testing. For the suppliers, the field testing indicated that the model met most of their expectations for planning, scheduling, and consistency of process; the suppliers indicated that the scope and duration of the audit were still of concern. The auditors' feedback was essentially positive; their principal area of concern was how to ensure objectivity, which the standardized templates improved, but did not guarantee.[3] The task group, representing the pharmaceutical companies, felt that the model was proven to be of sufficient quality that their companies could make valid decisions about suppliers based on the information in the test reports.

[3] These concerns have since been ameliorated through use of and experience with the model.

3 Enablers of the Process Model

In defining the process model, the task group determined very early that it would depend on several supporting technologies. We have earlier described how templates provide consistency and standardization in the audit process. In this section we describe some other enablers: the data collection tool that aids in execution of the audit; the audit repository, through which the results of supplier audits are made available on an ongoing basis to the pharmaceutical community; the framework for training auditors; and the use of metrics in the overall enterprise of supplier audits.

3.1 Data Collection Tool

The data collection tool provides a uniform basis for collecting data during an audit. It consists of two parts: an audit guide (AG) and an audit criteria checklist (ACC). Both of these parts are used in steps two through four of the process model.

The AG and the ACC are structured around a set of audit "areas." In the AG, each area is described through an "expectation" paragraph describing the qualities that the supplier should manifest. This is followed by a hierarchical breakdown of topics detailing the kind of evidence that the auditor should seek. In the parallel portions of the ACC, each element in the hierarchy maps to a question that the auditor is expected to answer. For each answer, the auditor is prompted for an indication of the objective evidence that supports his or her answer. The audit areas, along with brief examples of the "expectations," are below:

- quality system: all elements of quality control
- project management: formal planning methods
- design/development methodology: for example, written and documented software methodology, or written controls
- testing: efficient testing methods and technology
- configuration management: methods for configuration, change, and version management
- manufacturing: procedures for releases, supplier and subcontractor management
- documentation and records management: responsibility for generating, maintaining, and controlling documents

- security: policies and procedures for security administration, use of approved tools, virus detection, backup and recovery
- training and education: formal system to enable all personnel to perform assigned functions
- maintenance: support organization and mechanisms to assist customers
- date calculations:[4] correct calculation of leap years; proper exchange of date-related information

3.2 Audit Repository

The development of a rigorous and standardized audit process, and the existence of audit reports with confidential information, implies the need for a rigorous and standardized mechanism for storing and sharing this information. This need led to the creation by PDA of a central repository for audit reports and their accompanying data.

The repository, administered through the Audit Repository Center (ARC), functions as a third party, acting as a neutral agent between clients and suppliers. ARC is privately held, but is licensed by PDA and acts as an extension of PDA. ARC is the custodian for all of the evaluation information for the pharmaceutical industry. ARC ensures that audits submitted to the repository are executed by qualified auditors; all audits are subject to quality review by ARC.

Subscription to the repository is open to all industries. In most cases, a subscriber is an FDA-regulated organization that agrees to the terms and conditions of confidentiality, and who has pre-qualified as a business NOT in competition with computer technology suppliers or service providers.[5] Suppliers who wish to have their audit data made available to their clients may also join the repository as a participating supplier.

Subscribers must meet the requirements for subscription. They are screened via a two-step process. All applicants must first complete an initial application. After a review, the applicants are then contacted and enter into a subscription agreement with ARC. Subscription agreements require subscribers to indemnify that they are in fact not affiliated with the manufacture, production, retail, or marketing of computer products or services.

The repository functions by retention of the original copies of documents (i.e., the full reports, auditor qualifications, supporting audit data) and distribution of "true" copies of them to its subscribers. Reports are assigned an audit number prior to the audit. When an audit has been closed out, the lead auditor submits the report and supporting data to the repository.

---

[4] Y2K concerns of the task group forced the inclusion of inquires about date management in products provided by the suppliers. This line of inquiry has since been dropped in all audit activities.

[5] This is not a requirement, however, because ARC subscription is open to all industries.

Through ARC, the audit package is reviewed for PDA process conformity, legibility, grammar, and informational consistency. The original audit package is placed in an archive, and copies in electronic form are stored on a secure server.

Reports are distributed only after an authorized request has been received. An authorized request must be either a formal letter or a Web request; Web requests require a user ID and a password. When a user is found to be a qualified subscriber, no electronic data is transferred via the Web; reports are distributed only in hard copy and in sealed CD-ROM/PDF format. All hard copy reports and CD-ROMs are serialized with tracked delivery codes.

ARC also provides a refresh questionnaire to all suppliers whose audit data is one year old. The questionnaire is completed by the supplier and posted with the audit data that is made available to subscribers.

3.3 Auditor Training

PDA also defined a mechanism for auditor training and qualification, carried out by the Technology Research Institute in Baltimore. The process model sets forth an auditor training and education framework that describes the requirements for auditors and the scoring process that is used in qualifying them for entry into the program. These scores are based on experience, professional background, experience in quality methods, and similar factors. The model also sets out the syllabus for the auditor training program.

As of this writing, there are 92 qualified auditors, representing pharmaceutical companies, the European Union, and third-party auditors. (Third-party auditors make up nearly two-thirds of the total.)

The relationship between the auditor training program and the rest of the PDA audit program is shown in Figure 1.

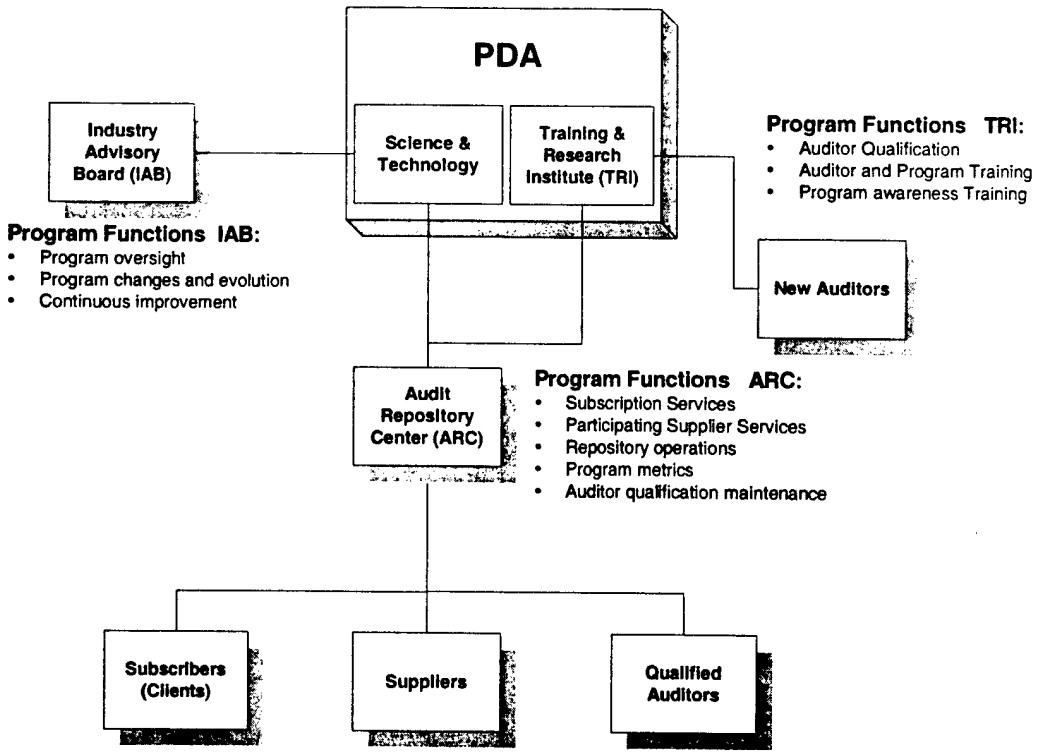


Figure 1: PDA Audit Program Organization

3.4 Metrics

The task group defined seven areas in which metrics should be collected:

- auditor performance
- process performance
- auditor training effectiveness
- data collection tools (i.e., ACC and AG)
- utility of audit results
- repository performance
- quality of audit results

For each area, measures were defined that permit objective assessment. For the first five areas, a questionnaire was developed to be completed by the audit participants. The questionnaire includes a list of several questions, each of which can be rated by level of agreement (e.g., "strongly agree...strongly disagree") and by level of importance (e.g., "not important ... very important"). For the remaining two areas, metrics are gathered from data that is intrinsic to the operation of the repository. In all cases, the metric data is maintained in the repository, to be reported to clients, suppliers, and PDA.

4 Results to Date

The initial rollout of the audit process by PDA occurred in March, 1999, with the subsequent opening of ARC in June, 1999. The essential industry infrastructure for education and process measurement became fully functional in January, 2000. Not until six months later did the first subscriber appear, with three more joining in the next quarter, and with the first actual audit occurring in the summer of 2000. The root causes of the slow launch of the program are attributed to the nature of the conservative FDA-regulated industry. The program's value to the industry was obvious from the initial analysis, but change is painful for a conservative industry where reactive behaviors are often driven by FDA proclamations and actions against regulated establishments. As it happened, the auditors themselves were important for managing change and gaining acceptance by regulated companies and external service providers.

A concerted effort was made to provide two levels of training to all stakeholders in the program. One form of this training was at the awareness level, to provide an overview of program components and operations for all stakeholders. The second form of training was directed at auditor qualification to provide specific instructions for planning, executing, and documenting audits, along with instructions on interactions with ARC and PDA. Seasoned in the old ways of auditing, many auditors did not appreciate the need for such structure in education, or in the planning and execution of an audit.

All candidates for the role of auditor are expected to have some set of applicable credentials that testify to their core skill sets. These credentials confirmed that candidate auditors had the technical and auditing skills needed to execute a process-focused audit. About 30 auditors had been trained by August 2000; 82 were qualified by the end of 2000. Since the beginning of 2001 there have been a steady number of auditors available in the pool, averaging around 80 to 90. As new auditors are qualified, normal attrition and requalification failures sustain the steady number. The available pool is also limited by the requirement for software process knowledge, which is not always readily available in the domain of FDA-regulated establishments.

The majority of audits to date have been completed by a small subset of the total population of qualified auditors: some 14 auditors have done the 29 audits on file in ARC. Hence, there are roughly 60 auditors who are trained but have not conducted a program audit in the field. Analysis has shown that some of those individuals were only interested in learning more about process-directed audits, and never really intended to perform an audit themselves.

The first year 20 audits were scheduled; the results of 7 were accepted into the repository.[6] The second year 30 were scheduled; 13 reports were accepted into the repository. In 2002, 16 audits were scheduled, 11 were completed, and 9 others were in process.

4.1 Experiences

The work so far has revealed that the least problematic audits are those requested by a supplier, in contrast to audits requested by an FDA-regulated subscriber. Supplier cooperation in making the resources available and ensuring clear communication of factual information appears to be the principal reason for observed efficiencies. By contrast, when an FDA-regulated subscriber sponsors an audit on a particular supplier, the supplier has the reasonable concern that the regulator (FDA) or a regulated establishment (other FDA-regulated companies) may infer quality problems if the supplier becomes enmeshed in a "cannot validate" determination by the audit sponsor. In the same vein, when a supplier requests a self-sponsored audit, ARC is in a unique position to educate the supplier about the process they are about to undergo. When an FDA-regulated subscriber sponsors an audit, the supplier may not be as well informed about the audit process. Sponsors apparently are not consistent in fulfilling this educational duty to the supplier when facilitating their coordination role. Given normal patterns of behavior, it may easily take longer to educate the supplier's personnel about the value of these audits.

The team had originally expected that the most commonly used technology products would result in the highest demand for audit information and that these companies consequently would be audited first, with these audits most likely sponsored by the supplier. In actuality, the first-year selection of the audits was driven by the FDA-regulated subscribers: submission of initial audits into ARC came from the subscriber community and not the supplier community. Incentives were given to subscribers in order to facilitate population of audit holdings in ARC (e.g., "the more you put in, the more credits/coupons you get"). This strategy, it turns out, had a limited effect. In the end, of 21 evaluations submitted to ARC (18 sponsored by subscribers), 11 of the subscriber-sponsored audits were not requested by any FDA-regulated subscriber. This may have been due to perceived need by the individual subscriber and not the FDA-regulated community. Incentives offered to all suppliers to participate (with several major suppliers accepting) had positive effects on the subscriber community and were well received.

---

[6] Some results do not get into the repository because they are not submitted, others because they are not accepted by ARC; for example, a supplier may have had input from their legal department, a pharmaceutical company may have decided against entering the results on behalf of a supplier (although the supplier can override that decision and put it in anyway if they are a subscriber), or a supplier may choose not to submit.

Initially there were some concerns over the scope and duration of the audits, but many of these concerns diminished as the audits proceeded. Scope issues, as it turned out, were limited to global companies where technology components are made at various sites and then assembled at one location. Scope in these situations had to include all sites, which required the auditor to go to all the sites to look at the production of the individual units. Alternatively, some situations required the coordination of several auditors located close to the target sites. Interestingly, some companies operated each site differently, resulting in a disparity of practices reflecting the culture of each site and not the international company. For example, in one instance a company unit in Texas assumed that their Paris site was following Texas procedures when in fact they were not. Separate data collection efforts also require more time to assemble a single large report for a global company.

Today the audits are largely used as a quality assessment supplement to the overall supplier evaluation; the audit demonstrates a good faith effort in acquiring marketplace technologies. Nearly all subscribers are renewing their subscriptions because they have found that the audits have value, resulting in reduced resource time for collecting data and more time for comprehensive analysis. This is in spite of the fact that the regulatory atmosphere is not as strong now as it was when the process was created. Certainly, a conservative industry that reacts positively to FDA actions would make greater use of the repository if the FDA were more active in due diligence with suppliers. Participating suppliers encourage their customers to use the ARC repository, thus reducing their overhead in entertaining numerous and diverse audits by individual FDA-regulated customers, as consistency of data collection and secure sharing of the data facilitates creating information once and reusing it multiple times. In its third year now, it may take several more years before ARC is up to the level where it is fully supported and used by the FDA-regulated industry in satisfying both the regulatory expectations and IT needs and evolving to sustain integration with emerging IT concepts, changing paradigms in the use of COTS technologies, and emerging e-record/e-signature laws. Other similar businesses (e.g., UL and Dun & Bradstreet) have also taken several years to become established entities in serving a general need.

Some issues of trust persist within FDA-regulated establishments. There may be internal management directives that do not allow an outside party to collect data for the company, or there may be an internal audit staff that intends to sustain itself. Contrasting with this, legal counsel has stated that it prefers that audits be outsourced and in-house personnel not used, thus reducing the company's liability in case of litigation. Some companies were motivated to push audit responsibility out to the supplier community and preferred the ability to subscribe to a service.

4.2 Benefits

A number of improvement opportunities were identified early in the project through the use of survey techniques. These derived benefits are summarized here in a "before and after" format to illustrate the program benefits that have been realized for the industry.

Table 1: Benefits for Suppliers

Before	**After**
Disparity in audit process, data collection, reporting, and follow-up. The disparity was observed both internally (divisional differences within a company) and externally (differences between companies).	Standardized process that suppliers can plan for (a letter of introduction, a formal schedule, information on what will be examined, a defined scope)
Great diversity between auditors; various checklists and auditing styles	Suppliers call ARC after the audit to say they appreciated the auditor's work
Auditor judgment as part of the audit reporting	Auditor responsible for data collection only. Judgment removed and returned to the customer domain.
Many audits per year, as many as 50	One audit every one to two years with secure sharing of information
Inability to use audits as a marketing tool	Marketing strategies can be built around shared audit information.
Limited utility of audit information to support internal improvement processes	Audit information supports process improvement initiatives.

Table 2: Benefits for the FDA

Before	After
Little if any documented programs in regulated companies for consistent auditing practices	Defined six-step process, data collection tool, templates for consistent reporting of information, education and metrics infrastructure to evolve program
Difficulty in assessing audit practices	A current good practice against which to examine company in-house audit procedures. If a company subscribes to the PDA program, the FDA inspector is assured of reliable data collection activities.
Numerous FDA citations	No FDA citations on program to date.

Table 3: Benefits for Subscribers

Before	After
Diversity of internal procedures	Economy in not having every division or site have its own procedure and teams. It makes for an easy way to standardize within the subscriber organization a one-stop service for scheduling, executing, and funding an audit.
Disparity among FDA-regulated companies	Industry standard for audit consistency and data collection, facilitating sharing of audit data that can be used by FDA-regulated companies
Complexity in staffing and managing huge audit loads required to support technology projects	Reduced staffing and coordinated management of audits both within companies and among companies
Start-to-finish audit process duration on the scale of months	Start-to-finish audit process for acquiring and analyzing audit data on file in ARC reduced to the scale of days, making for more agile supplier evaluation supporting procurement and COTS acquisition practices

One major pharmaceutical company has indicated that its audit costs went from about $750K/yr for funding audits to about $350K the first year, then $120K subsequently. Through the use of trusted third-party qualified auditors and ARC, two full time employees were able to manage audit requests, complete paperwork, and analyze the results for supporting yearly technology project needs, with approximately 40-50 audits per year per person. Previously the company had needed 25 people at each of its manufacturing sites.

There has been a positive effect on the computing environments that FDA-regulated companies engineer using what they get from their suppliers. Knowing about the supplier's behavior early in the project can save considerable time and effort in resources expended to deal with problem suppliers in the course of the project. Suppliers also get information on how their product will be used, so the supplier can better test it for the FDA-regulated company's needs. Thus the process is giving the companies the information they need to begin to manage risks and thereby ensure better quality for the computing solutions that depend on the supplier. In addition, the information can be used for the supplier selection process, and suppliers have used the data to improve their own development system.

5 Lessons Learned

Two principal classes of lessons were learned from this experience. The first set of lessons focuses on the result, that is, the audit method itself. The second set of lessons concerns the work of the committee in developing that process.

5.1 Lessons About the Audit Method

1. The PDA audit is a process examination, not a product examination.
This represents a shift in focus on how the audits were done historically. Previously, most audits were dominated by a product focus: requirements, design, and test procedures for a particular product and version. The new focus of an audit is not to investigate specific features and attributes of the product, but instead to examine the process for creating that product. This new focus is not entirely embraced by everyone within the PDA community; some customers are still demanding audits of products. But suppliers have now begun to refuse such requests, and the process-focused audit is gaining word-of-mouth acceptance by suppliers.

2. The auditor's job must be solely to collect data, not to render a judgment.
The new audit process separates judgment from data collection: auditors are now removed from making judgment, and merely report facts. The major benefit of this approach is that the subscriber now accepts the responsibility for reviewing and analyzing the results, based upon the evidence presented through the audit. It is the customer's responsibility to judge, not the auditor's. (This issue was singled out in recent surveys as one of the three main benefits of the new audit process, the other two being reduced cost and increased confidentiality.)[7]

3. Auditors must be qualified to investigate software processes.
Those auditors who initially came without a software background – using their previous background in other kinds of auditing – frustrated their audit subjects because that background did not always translate to software.

[7] It must be noted that this approach has also resulted in some discomfort and criticism. At least some of the criticism can be attributed to the "not invented here" syndrome. But others feel that charging both the suppliers and the companies is inappropriate. The PDA response is that this is done to get universal buy-in, and also because the infrastructure must be self-perpetuating.

4. Customers must have confidence in the sanctity of the audit information.
It is imperative that the information gained through an audit be maintained with integrity, security, and confidentiality. So far, this has been done successfully. The subscription policy supports this integrity: the application asks what an applicant will do with the information, there is a legal subscription agreement, and the applicant must attest to the validity of his or her interest in the information. ARC takes numerous pains to ensure security. For instance, submitters lock the submitted files with a password that is never given to ARC. (Note that confidence in this sense is distinct from any notion of industrial espionage. The information in the repository would probably not be of much use for that purpose, since it is an assessment of the process, not details of a product. But its value is no less significant for the PDA community.)

5. Standardized methods of auditor training are necessary.

The standardization of auditor training has proven invaluable, as have the requirements for a quality review of the auditor's work. These standards are the major factor in providing a consistent data package for the subscriber. Prescreening ensures that the candidate auditors have appropriate skills and domain knowledge. Also, the look and feel of the audit reports is consistent, so the subscriber can depend on the nature of the report contents and can know which section to consult to find a given item. Note that the goal of the standardization and review is only to make the results independent of which auditor performs the audit; auditors are still free to use a style with which they are familiar and comfortable.

6. It is imperative that the audit process be affordable for all.

A major goal in devising the new audit process was to build the subscription structure in a way that was economically level, so that everyone could afford to participate, regardless of the size of the supplier or pharmaceutical company. The possibility of selling an audit by its "relative worth" (i.e., regardless of the qualities of the subscriber) was considered at one point, but this was rejected in favor of the "flat" subscription scheme that is now in place.

5.2 Lessons About the Committee's Work

7. Committee members must have access to the decision makers.

The nature of PDA was a factor in the slow start for the work of the committee. Because PDA is a professional organization, not an industry organization, members represent themselves, not their companies, and are not empowered to bring change into their companies. Sponsorship by the decision makers within each company is critical, and the success that is now oc-

curring is largely based on the growing presence of such sponsorship. Without it, all of the committee's work could disappear.

8. Surveys are a useful starting point for developing a method such as the PDA audit.

The committee used surveys to great benefit to bring to the surface issues in the stakeholder community. For example, the idea of companies sharing audits had always encountered resistance in the form of restraint-of-trade complaints. However, surveys revealed that the real issue turned out to be in the supplier domain (i.e., the number of ways that different companies would participate to accomplish that goal). But the suppliers did not have any problems with the restraint-of-trade issue, so long as their competitors would not have access to the confidential information.

Another issue resolved by survey was the question: after the information is gathered, whose property is it? The pharmaceutical companies wanted it to be theirs, but the suppliers were adamant that the information was theirs. The survey that went to the FDA produced one of the more surprising results: all of the FDA inspectors simply wanted to know what the procedures were. The surveys also provided insight with regard to the repository, revisit policies, and information refreshment.

5.3 Other Lessons

In addition to these, there were other more general lessons whose value was affirmed by this experience. Thus, the decision to partition the effort into working groups was a good one. The working groups met once every other month for the first half-year, then once a month for roughly a year. Each meeting was for one day, and working groups were encouraged to have additional individual meetings as needed. PDA provided the meeting space and helped with the rollout. The committee also participated in PDA annual and semi-annual meetings.

Finally, as has been noted in several previous sections of this case study, metrics were also seen as fundamental for such an effort, especially during the initial stages.

6 Conclusion

One of the goals of this project was to establish an organizational assessment program for the FDA-regulated client that had a technology process focus but did not waste valuable resources rediscovering an assessment method. The committee concentrated its research on experiences and programs both within the FDA-regulated industry and external to it. The resulting program was assembled from successful features of numerous functional supplier assessment practices. The unique features of this program are: (1) domain independence, (2) a functional repository that meets the security concerns of all stakeholders, (3) a supporting infrastructure for continuous improvement (training and qualification of auditors, ensured refresh of assessment data, operational metrics, and oversight by an independent board), and (4) deliberate separation of audit process from data collection tools.

The potential value of this program to prospective subscribers external to the FDA-regulated industry (e.g., government, defense, and other private industries) is quite high. The benefits of adopting the program should prove immediate, because: (1) there is little need to spend development time to create a program that is industry specific, (2) one gains immediate access to current report data in the repository holdings, (3) there is increasing cross-industry value of the program, thus increasing the repository holdings, and (4) by layering data collection needs on top of the common data collection tools, the user can leverage program modularity for either industry-specific or even subscriber-specific issues.

Failure to adopt the program could result in an inefficient use of valuable resources and lost time to build and calibrate a program specialized to a specific industry. Time and resources spent on such a task can now be redirected to integrate knowledge of a supplier's technology process into technology acquisition practices. Using such knowledge when purchasing COTS products can reduce procurement, project, and technology risks.

Glossary

Annual Audit Requirement Levels	number of audits a company must undergo in a year
Audit	Audit performed in accordance with PDA Technical Report No. 32 and brokered by ARC for participating suppliers or supplied by subscribers as required by their level of subscription
Audit Data Package	See audit reports.
Audit Reports	The audit data package for audits completed using the audit process and verified by ARC to meet the requirements of PDA Technical Report No. 32. This includes, at a minimum, the information defined in Section 40-070 of PDA Technical Report No. 32.
Audited Supplier	A supplier audited by a subscriber in accordance with the PDA process where the audit report is placed in the repository by the subscriber
Brokered Audit	An audit of a participating supplier that is requested and financed by that participating supplier and coordinated by ARC
Contribution Requirement	number of audits a subscriber must contribute
Participating Supplier	A supplier of computer technology or services to the pharmaceutical industry that chooses to participate in the PDA audit process by sponsoring the implementation of an independent audit of its activities for submittal to ARC for distribution to subscribers.
Process	The PDA supplier auditing and qualification process as described in PDA Technical Report No. 32.
Subscriber	A pharmaceutical industry company-whose business lines do not include the development, distribution, resale or modification of computer products-that wishes to share supplier audit information

within the industry.

Subscription — The services purchased by a subscriber or participating supplier via a signed agreement with ARC. The subscription agreement defines, among other things, the audit entitlement and contribution requirement as well as fees for audits above the entitlement and discounts for audits in excess of the contribution requirement.

Subscription Audit Entitlement — number of audits of participating suppliers that subscribers can examine

Supplier — A supplier of computer technology or services to the pharmaceutical industry that chooses to participate in the process either as a participating supplier or by release of its PDA process audit data to a subscriber for retention in the repository for distribution

References

[ERCI 88] ERC International. *Vertical Slice Verification Techniques* (ERCI-88/1001). Fairfax, VA: ERC International, 1988.

[Hawkins 88] Hawkins, F.; Johnson, L. H.; Liner, L. T.; & Putnam, C. H. *Performance-Based Inspection Techniques* (NUREG/CR-5151; SAIC-88/3014). Washington, DC: U.S. Nuclear Regulatory Commission, 1988.

[PDA 99] Parenteral Drug Association. *Auditing of Suppliers Providing Computer Products and Services for Regulated Pharmaceutical Operations* (PDA Technical Report No. 32). Bethesda, MD: PDA, Inc., 1999.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	May 2003	Final

4. TITLE AND SUBTITLE
Case Study: Computer Supplier Evaluation Practices of the Parenteral Drug Association (PDA)

5. FUNDING NUMBERS
F19628-00-C-0003

6. AUTHOR(S)
David Carney, Harvey Greenawalt, George Grigonis, Patricia Oberndorf

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

8. PERFORMING ORGANIZATION REPORT NUMBER
CMU/SEI-2003-TR-011

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
HQ ESC/XPK
5 Eglin Street
Hanscom AFB, MA 01731-2116

10. SPONSORING/MONITORING AGENCY REPORT NUMBER
ESC-TR-2003-011

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT
Unclassified/Unlimited, DTIC, NTIS

12B DISTRIBUTION CODE

13. ABSTRACT (MAXIMUM 200 WORDS)

This case study describes the development of a method for evaluating computer and software suppliers for the pharmaceutical industry. The study describes the role of government regulation within the industry and the need for standardized audits of computer and software suppliers.

The audit method consists of six steps: initiation, pre-work, auditing, observations and reporting, decision, and follow-up. Each of these steps is described in detail, as are several features of the method: a data collection tool, an audit repository, and extensive auditor training supervised by an industry-regulated oversight agency.

Finally, the report describes the benefits of this audit method, together with a set of lessons learned about the audit of computer and software suppliers.

14. SUBJECT TERMS
COTS software, evaluation processes, supplier evaluation, supplier audit, PDA

15. NUMBER OF PAGES
45

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL