



THE SECURITY AUDIT PROGRAM

A How-To Guide and
Model Instrument
for Adaptation to
Local Standards, Policies,
and Procedures

**U.S. Department of Justice
National Institute of Corrections
320 First Street, NW
Washington, DC 20534**

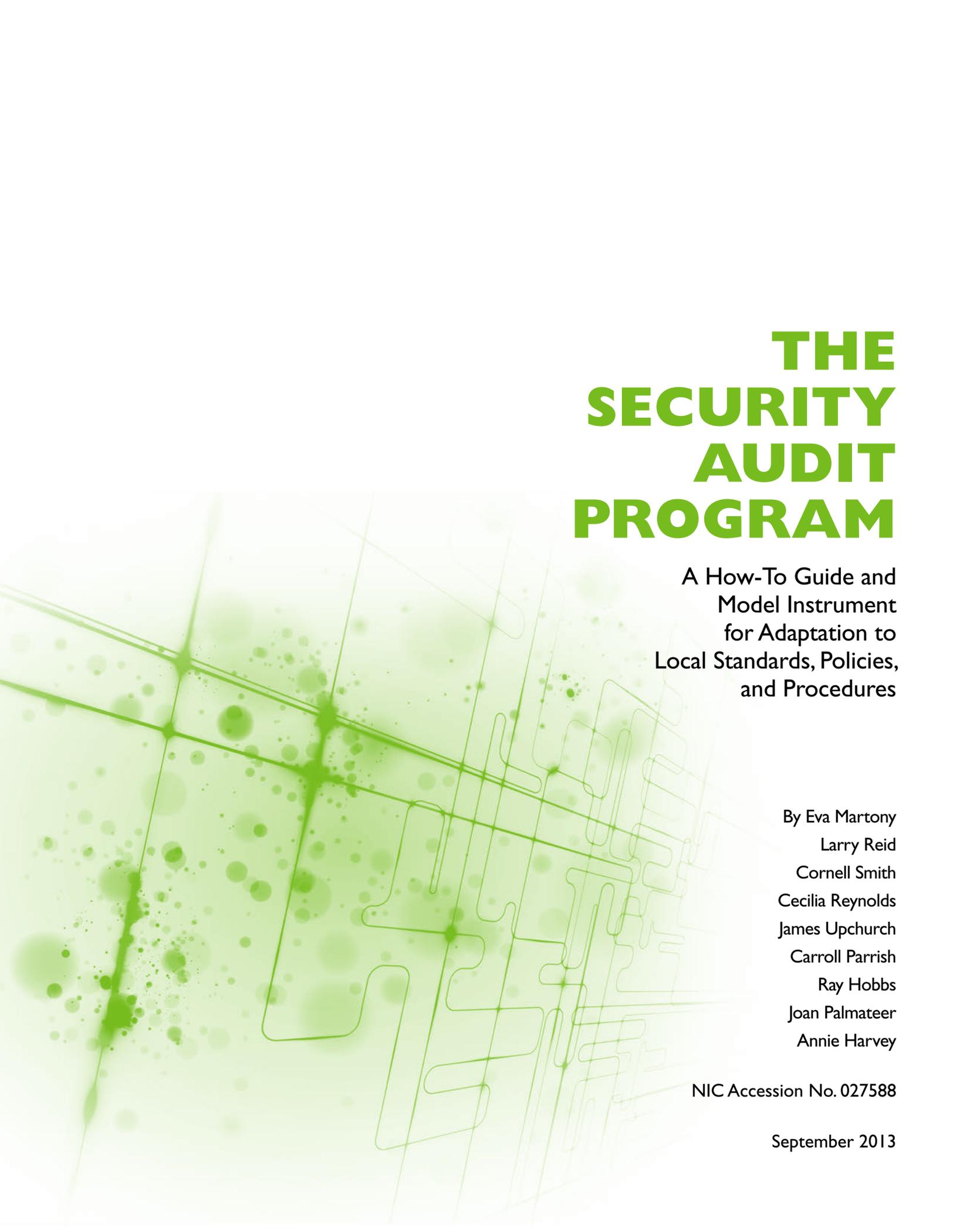
Robert M. Brown Jr
Acting Director

Harry Fenstermaker
Acting Deputy Director

BeLinda Watson
Chief, Prisons Division

Wayne Hill
Project Manager

National Institute of Corrections
www.nicic.gov



THE SECURITY AUDIT PROGRAM

A How-To Guide and
Model Instrument
for Adaptation to
Local Standards, Policies,
and Procedures

By Eva Martony
Larry Reid
Cornell Smith
Cecilia Reynolds
James Upchurch
Carroll Parrish
Ray Hobbs
Joan Palmateer
Annie Harvey

NIC Accession No. 027588

September 2013

The National Institute of Corrections values your feedback. Please follow the link below to complete a user feedback survey about this publication. Your responses will be used to assist us in continuing to provide you with high-quality learning and informational materials.

<http://NICIC.gov/Go/UserFeedback>

Points of view or opinions stated in this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice. The National Institute of Corrections reserves the right to reproduce, publish, translate, or otherwise use and to authorize others to publish and use all or any part of the copyrighted material contained in this publication.

INTRODUCTION: SECURITY AUDITS

A *security audit* is a process for determining the extent to which policy, procedure, standards, and practice combine to provide a safe and secure institutional environment. Included in this process is a detailed evaluation of every major aspect of an institution's security program.

The work of the security audit may be best described as *risk assessment*. The function of a risk assessment is to determine the likelihood of a significant security problem or vulnerability to injury, escape, disruption, or destruction of property because of the inadequacy of policy, procedure, physical plant, or performance. A security audit or risk assessment is the process of determining the risk remaining after all the normal management safeguards have been applied, including clarity of policy, procedures, and post orders; training; physical plant accommodation; and daily supervisory activities.

Moreover, a quality security audit program allows for all of the detailed assessment described above but does so in a nonadversarial manner that creates a “win–win” opportunity for everyone involved. This includes agency and institutional management, supervisors at all levels, and line staff.

Avoiding an “I gotcha” philosophy in favor of a cooperative look at how to strengthen an institution's security posture eliminates the detrimental impact of unhealthy competition and divisiveness. Staff at all levels working together is the most effective way to bring to life an overall “security mindset” within the facility!

Protection of the public, staff, and inmates is the primary mission of any prison system. Experience has proven that the development and implementation of a comprehensive security audit program is a major step in reducing the risks that are endemic in prison operation. This document can help achieve that end.

CONTENTS

- Chapter I. The Development of a Security Audit Program..... 1
 - Attachment 1: Audit Instrument Report Example 9
 - Attachment 2: Tabular Security Audit Instrument 13
- Chapter II. How to Perform a Security Audit..... 19
- Chapter III. The Audit Report..... 31
 - Attachment 3: Department of Corrections Security Legislative Report..... 37
- Chapter IV. The Security Audit Instrument 39

Audit Instrument:

- Section 01: Armory/Arsenal..... 43
- Section 02: Control Centers/Communications..... 48
- Section 03: Hazardous Materials Management..... 54
- Section 04: Inmate Counts..... 58
- Section 05: Controlled Movement (Internal and External) 61
- Section 06: Inmate Work Assignments 67
- Section 07: Key Control 71
- Section 08: Perimeter Security..... 82
- Section 09: Physical Plant..... 93
- Section 10: Searches 98
- Section 11: Segregation (Special Management)..... 106
- Section 12: Tools and Sensitive Item Control 113

Addendum Guidelines:

- Guideline A: Use of Force 122
- Guideline B: Emergency Plans 125
- Guideline C: Security Inspections..... 129

CHAPTER I.

THE DEVELOPMENT OF A SECURITY AUDIT PROGRAM

The past 20 years have been characterized by rapid growth in prison construction and an accelerated evolution in prison and jail design. Perimeter barriers, locking systems, video and communication technology, and alert systems have all significantly improved. These improvements have resulted in more efficient, effective operations and enhanced safety of staff, inmates, and the community. Good sightlines integrated with sound security hardware and reliable technology have become the hallmarks of efficient, safe, secure, and humane correctional housing. Such enhancements balance cost-effectiveness, ease of maintenance, and efficient use of staff resources. Without question, modern prison designs represent significant improvements over many of the models that preceded them.

As important as these improvements are, however, they cannot by themselves provide a safe, secure, and humane environment. They are only a part of what is necessary to ensure a sound security plan, program, and operation. The most innovative design and advanced technology cannot substitute for well-trained staff and good security practices that are based in comprehensive security policies, procedures, regulations, and rules that are clearly written, standardized, and fully implemented. Even then, without a well-planned, comprehensive monitoring program, effective security practices cannot be sustained over the long term.

*You get what you inspect,
not what you expect.*

The Security Audit Program

A nationwide review of after-action reports of escapes, staff assaults, hostage situations, disturbances, and other serious problems reveals few instances in which malfunctioning locks or electronic detection systems, insufficient razor wire, or other deficiencies in physical plant or technology were responsible. Rather, most serious security breaches occurred because one or more staff members took a “shortcut,” did not know what was expected of them, or simply failed to follow established security procedures. Though weaknesses in the physical plant may have contributed to the problem, it was usually the failure of staff to attend to business that was at the heart of the incident. In other words, “people-system failures,” not “physical-system failures,” account for most security breakdowns.

This unfortunate reality points to the need to establish a comprehensive monitoring program. An adage that is familiar in security circles, “You get what you *inspect*, not what you *expect*,” or stated

another way, “Staff will *respect* what you *inspect*,” is certainly true; it underscores the fact that line staff will view what the “boss” pays attention to as important. It is through consistent monitoring that the agency leaders and institution administrators/managers affirm the importance of sound standards, policies, procedures, and security practices.

No longer can institutions be operated as separate and autonomous “kingdoms” in which sound, commonly held security principles are ignored. Increasing public sensitivity to correctional issues, litigation against corrections officials, increasing size and complexity of facilities, existing and emerging national standards, and a growing knowledge base of professional practice require that correctional systems and their individual institutions operate within established and broadly held security standards. It is through a program of security monitoring/auditing that an agency ensures that such practices continue in place, without compromise.

Definition

“Security audit” is a process for determining the extent to which policies, procedures, standards, and practices combine to ensure a safe and secure institutional environment.

Types of Audits

There are three types of audits in correctional facilities through which aspects of security operations are monitored. The first, an audit of standards, is based on American Correctional Association (ACA) accreditation standards or is a self-audit based on similar standards adopted by an agency or association of agencies. A standards audit is a well-accepted and valid way of assessing the overall operation of a correctional facility. However, it lacks the comprehensiveness, intensity, and security focus that are necessary to identify numerous elements of risk to which many security operations are vulnerable.

The second type of audit, the policy audit, seeks to ascertain whether or not centrally mandated policies and related procedures are in place. Such audits are valid in determining institutional compliance with agency policy but generally fall short of identifying weaknesses in the operation caused by deficiencies in training, supervision, and/or practice that may create risk. A policy audit of key control, for example, may determine that policies and procedures are in place, but this type of audit will not often determine if they are being carried out in practice or that essential procedures beyond those mandated by agency policies are appropriate. For example, a policy audit may find an institution to be in compliance with a policy requiring the warden to authorize the assignment of permanent (take-home) keys. But such a finding does not speak to *which* keys are taken home by *whom*, and there may be literally hundreds of such sets assigned that are not routinely inventoried. Such a condition may suggest a key control system that is out of control while having in place each required policy.

The third, the security audit, focuses on security operations. Although standards and policies are important aspects of such audits, the primary focus is the security systems and their operational implementation on a daily basis. This audit is a “where the rubber meets the road” experience that, when properly conducted by persons who are familiar with security principles, identifies weaknesses in the program that create risks to safety and security. Although standards and policy audits are important, the security audit is essential to identifying “slippage” or “cracks” where policy and procedure enhancements are necessary. Such subtle changes over time as new staff entering the institution workforce; experienced staff becoming complacent; weakened supervision as new, inexperienced supervisors are promoted; aging physical plant and equipment; addition of new buildings and equipment; and expanded use of inmate workers can render policies and procedures dangerously deficient and ineffective. Security auditing is a real-time process.

Outcome

The *outcome* of the security audit may be best described as a “**risk assessment**,” which may be defined in this context as “a determination of the likelihood of significant safety or security problems or vulnerabilities to injury, escape, disruption, or destruction of property because of the inadequacy of policy, procedure, and/or staff performance.” Risk assessment is the process of determining the risk remaining *after* all the normal management and operational safeguards have been applied, including clarity of all instructional documents, training, and daily supervisory activities. Factors that create such risks may include poorly designed policies, inadequate procedures, overlooked standards, a facility design inappropriate to a changed inmate profile, inadequate training, or staff inattention to the requirements of their positions.

The security audit is accomplished through intensive observation, discussions with staff, and the testing of internal controls. In a security audit program, auditors address five basic questions that, when objectively answered, provide an assessment of risk and vulnerability with recommendations for rapid correction of the condition of risk. These questions are:

- What is the current condition? (a snapshot of reality)
- What should it be? (standards, policies, criteria, etc.)
- Why is it important? (probable effect or impact of the current condition)
- How did this condition come about? (cause)
- What will correct the problem? (recommendation)

To address these questions systematically, the security auditors must determine the adequacy of policies and procedures, observe staff practices as related to expectations, examine the staff’s knowledge of job requirements, and inspect the facility’s equipment and hardware. Periodic security audits will strengthen the entire operation of the institution.

Reasons for a Security Audit System

Why should a correctional agency have a comprehensive security audit program? The benefits to the agency, institution, and community are many. Several are discussed here.

A security audit identifies weaknesses, deficiencies, and areas of vulnerability in the institution's operations.

Without a comprehensive and systematic review of facilities, operations, and equipment, it is unlikely that weaknesses and deficiencies will be reliably identified before they become problematic. Inability to “see the forest for the trees” inhibits institutional leaders’ ability to identify weaknesses, deficiencies, and vulnerabilities without specific mechanisms that force their attention to that level. Staff familiarity with their surroundings is both a “blessing” and a “curse”: a blessing as it contributes to efficiency of performance but a curse as it contributes to complacency and development of shortcuts that create risk.

A security audit assesses compliance with agency- and institution-endorsed standards, policies, and procedures.

It is only through targeted review and observation of policies, procedures, practices, and outcomes that leadership can assure that expectations are being met. Without an audit program, deficiencies in the security operation are often discovered only as inmates test the system through assaults, escapes, or other undesirable activities. Monitoring over time assures leaders of compliance, particularly as the operation becomes self-monitoring in anticipation of monitoring by the organizational leadership.

A security audit identifies equipment, locking mechanisms, tool and key systems, and other physical safeguards and control systems that are inoperable, inappropriate, or inadequate.

During NIC's *Conducting Security Audits and Emergency Preparedness Assessment* seminars, in which participants are trained through participation in audits and assessments, serious problems are frequently identified. Emergency keys that no longer fit locks because of wear to the lock or changing of the lock, airpack breathing devices that are inoperable, policies and post orders that are inaccurate and ineffective because of facility modifications, perimeter intrusion systems that are shut down or inoperable, and tool control systems that do not fully account for tools are but a few of the serious issues that have been frequently identified. Monitoring systems make it easier to detect and correct such security breakdowns.

A security audit reviews the efficient and effective application of security resources.

It is not uncommon that temporary posts/assignments become permanent, critical but unpopular activities are abandoned, security standards or policies are compromised, or other “slippage”

occurs because of the press of everyday supervisory requirements or staff inattention. Auditing security operations identifies many such costly “loose ends” to the institution, both in manpower and in safety/security.

A security audit identifies and shares “best practices” throughout the agency.

Even as staff have the capacity to become complacent in performance, they also have the capacity to refine their activities to a point of vast improvement over the stated procedure or expectation. It is important to identify and recognize these initiatives and to share the resulting improvements with other parts of the organization. Failure to identify and reward initiative discourages further initiative. Conversely, recognizing initiative provides for and reinforces the positive role of the audit process to the staff subject to its scrutiny.

Essentials of the Security Audit Program

Security audits that “just happen” and are not part of an authorized, planned program designed to upgrade security operations are almost invariably met with resistance. Institutional managers often perceive that they have been singled out and therefore dispute and resent the findings. Several essentials form a foundation for an agency security audit program that will be viewed as legitimate and helpful.

Administrative Support

The first essential step in developing an audit program is to marshal the full support and participation of top administrators (central office and institution leaders) in planning and preparing for security audits. This support will make a critical difference in the response of institution staff to the audit process. Administrators can convey an audit intent that is helpful and nonthreatening in the following ways:

- Facility leaders clearly state their commitment to the audit program and their intent that it be a helpful tool to their staff.
- They clearly articulate audit objectives in terms that emphasize safety and security and focus on “what,” not “who.” They acknowledge that the audit will identify deficiencies but will not target staff.
- They clearly articulate behavioral and performance expectations for auditors and exercise care in selecting auditors who are knowledgeable and credible.
- They ensure that audit team members are thoroughly trained *before audit activities begin*.
- They review, clearly articulate, and reinforce the security standards against which institutional practices are measured.
- They commit to a “fresh eyes approach” that shows a willingness to take a new look at any and all policies, standards, and practices.

- They ensure that audit objectives include identification and communication of “best practices” as well as areas of vulnerability. They encourage the recognition of staff who are demonstrating sound security practices and awareness at verbal debriefings and in written reports.
- Leadership encourages the “celebration” of good safety and security findings and outcomes, fosters a learning environment in which the audit is a learning strategy, and prohibits condemnation of staff when weaknesses or deficiencies are identified.

When positive findings and results are celebrated and deficiencies are corrected with strengthened policies, standards, and practices, updated training, and enhanced supervision, staff will grow to accept and support the audit process. Their acceptance will be in a spirit like that of acceptance of an annual physical examination: perhaps inconvenient, but essential to their long-term betterment.

Security Audit Policy

The second essential step is the establishment of the authority and a mandate for security audits. At a minimum, the policy should address the nature of the program, including frequency of audits, whether audits are announced or unannounced, criteria for selection of auditors, training requirements for auditors, the type of audit report required, and the agency’s expectations regarding the institution’s response to the report. The security standards and security audit instrument that are authorized for application should be referenced by location and most recent date of revision.

The policy should address the type of audits that are required. Some jurisdictions mandate a combination of *internal* audits and *external* audits. Internal audits, those conducted by staff within an institution, are sometimes mandated between external audits, audits conducted by a team or staff from outside the institution. In other jurisdictions, internal audits are *preaudits* and are conducted by institution staff just before the external, agency audit.

Internal audits are not recommended as the sole audit activity. Internal auditors often find it difficult to objectively point out shortcomings by friends, coworkers, and supervisors. For that reason they lack credibility. In addition, they may not identify risks or vulnerabilities as they audit the conditions in which they work every day.

Conversely, external audits tend to be more objective and thorough. They may be announced or unannounced. An advantage of unannounced audits is that they examine the institution’s operations in conditions more closely approximating “normal.” An advantage of announced audits is that the institution has an opportunity to prepare and correct conditions that are known to be deficient before the audit occurs. Some jurisdictions have found a combination of announced and unannounced audits to be effective—a schedule of unannounced audits sometimes being established on a random basis.

A third approach to auditing is contracting with experts from outside the system or institution. This has the advantage of bringing expertise from a broader experience base and will normally be free of allegiances that get in the way of objectivity. Disadvantages of this approach include cost

and outside auditors' possible lack of knowledge of labor agreements, statutes, administrative philosophy, and the history and various nuances that make the agency what it is. Most jurisdictions contract with outside experts in exceptional circumstances when credibility and objectivity are essential and cannot or will not be perceived to be so in an agency-based audit.

Security Operations Standards

Essential to the development of a security audit program is the development of a manual of security operations standards against which various components of the security operations can be measured. Without it, the auditors are “shooting at moving targets” as varying interpretations, understandings, and/or perceptions of the agency standards get in the way of assessments of practice. The development of an agencywide security audit program provides an opportunity and a rationale for the establishment of such standards for review and buy-in by institution managers. The security audit standards of an agency and its institutions constitute the “bill of particulars” by which the agency and its institutions operate. The standards reflect the minimum level of acceptability for each component of security operations and, as such, are the gauge by which the security audit program measures security operations performance.

Security standards should be based in the mission of the agency/institution and incorporate:

- Agency/institution policies, post orders, and procedures.
- ACA security standards, as applicable.
- Best security practices as identified in discussion with security professionals and agency/institution experience.

Security standards should be adapted for application to various security/custody levels and subject to the review and input of all security managers and facility managers who will be required to comply with these standards.

Security Audit Instrument

Finally, a security audit instrument must be developed that is consistent with the security operations standards of the agency and guides the auditors as they conduct the audit. Consistent use of an instrument endorsed by the agency will go far in reducing charges by managers that they are being “targeted” or that their audit was unfair. Numerous examples of audit instruments are available for review by contacting security managers in other states and localities. These instruments can be helpful in reviewing/developing security standards and an audit instrument, as can the publication, *Guidelines for the Development of a Security Program*, available from ACA. Perhaps the most comprehensive institution security document in print, this document can serve as a working manual in developing an audit instrument. However, whatever tool or other example is used, like the instrument included in this document, the tool or example must be customized to the agency's mission, policies and procedures, and security standards to be effective. Ownership and buy-in by everyone involved are critical to a successful audit program.

It is important to recognize that, because standards differ from jurisdiction to jurisdiction, a universal comprehensive security audit instrument does not exist and, arguably, cannot be developed.

Security audit instruments may be in various formats. Generally, however, they fall into two basic types, the narrative instrument and the tabular instrument.

Narrative Instrument:

The narrative instrument lists points of review that represent the priority concerns of an agency as related to basic security topics (e.g., searches, visitation, key control). Following each point of review, there is generally space for the auditor to record observations or comments (see Attachment I).

For ease of use, this format is unsurpassed. However, it requires that the auditors be experienced security professionals because the points of review usually consist only of the priority concerns in the topical area and do not attempt to list all of the concerns. This format assumes that the auditor will observe other commonsense security matters and issues related to the listed points of review.

In addition, this format lends itself well to situations where auditors from outside the system, who are not familiar with agency-specific policies, procedures, or practices related to security, conduct the audit. It may also be preferred in an agency in which security standards have not been clearly articulated.

This audit format is less likely to produce a checklist in which auditors are focused on the format. Its use encourages and allows for constructive thinking and broader exploration of issues than does use of a tabular or checklist-type format.

A negative aspect of this format is that points of review may often lack reference to an established set of standards for security practices; however, this is by choice rather than necessity. In developing the instrument, each point of review can be identified in its relationship to Security Operations Standards; or, as in the tabular format, it can be assumed that all points of review are agency policy, if the agency so chooses.

Some may argue that this format does not generate a complete record of the security operation at the time of the audit, as may a tabular (checklist) format. Caution would suggest that *no* instrument generates such a complete record. The skill and knowledge of the auditors—not the instrument—determine the completeness of the assessment of the security operation. Finally, converting a narrative instrument to an action plan may be more cumbersome than with a tabular instrument, but it is likely to be more informative about the issues being addressed.

AUDIT INSTRUMENT REPORT EXAMPLE

NARRATIVE SECURITY AUDIT INSTRUMENT FORMAT

I4.01 There is written policy establishing an automation security workgroup to review all requests to grant inmates use of computers and computer technology as part of their work or study assignments.

Observation:

There is no computer security workgroup.

Recommendation:

Establishment of such a group with first mission to develop local policy and oversight procedures for inmate computer access.

I4.02 Knowledgeable staff audit all inmate computers at least quarterly to prevent abuse or unauthorized use of the systems.

Observation:

No such practice of computer review is in evidence.

Recommendation:

See I4.01.

Key Control

I6.01 A staff member is assigned to assist the locksmith and to provide backup assistance in the absence of the locksmith or during an institution emergency.

Observation:

Sgt. XXX is the only trained locksmith at the facility and is not currently on a pager for an emergency response.

Recommendation:

Select and train a backup locksmith for the facility and provide a pager for the current locksmith to facilitate his timely response to the facility in case of emergency.

AUDIT INSTRUMENT REPORT EXAMPLE (CONTINUED)

16.02 **There are a position description and current post orders that describe the duties and responsibilities of the locksmith and locksmith assistant.**

Observation:

The current locksmith, Sgt. XXX, is also responsible for tool control, pest control, and fire safety. These assignments encompass a vast area of responsibilities in the facility. There is no post order for these functions.

Recommendation:

Develop a post order that would clearly define the scope and parameters of this individual's duties and responsibilities within the institution.

Special Issue:

Sgt. XXX is an outstanding employee who has shown a high level of skill and commitment and should be commended for all the duties in the facility for which he is currently responsible. He created the lockshop, including use of his personal equipment for key cutting, pinning, stamping, etc. He created a fire-response capability of six inmates, trained them, and has carts with all response equipment immediately available. He also created on his computer a manual for evacuation codes, one of the most comprehensive specific documents this team has ever seen. Great job, great employee.

16.03 **All keys are returned to the issuing location at the end of the workday or when the employee to whom the keys were issued leaves the institution.**

Observation:

The team is concerned that the facility does not have a central area to issue facility keys to staff. They are issued from various areas within the facility to the staff assigned to the area. The concerns include accountability, noncurrent inventories, and broken or lost keys. Staff on units exchange keys, but they do not exchange key chits.

Recommendation:

Issue keys from central area such as Post # 1. Utilize the chit system.

For assignments, keys are exchanged and do not leave the post. Procedures should explain how to exchange chits. In units where keys are exchanged from one staff member to another, the exchange should be noted on the shift log with the number of keys exchanged and staff key chits maintained in the officers' area.

AUDIT INSTRUMENT REPORT EXAMPLE (CONTINUED)

-
- 16.04** A record of the issuance of restricted keys is maintained, bearing the key ring number, date, time of issue and return, the person to whom issued, the purpose of the issue, and the person authorizing the issue.

Observation:

The locksmith's two sets of duty keys (highly restricted) are issued and turned in at Post #1. No procedure is in place for preventing these keys from being issued to anyone who requests them.

Recommendation:

The use of a sequence lock for these sets and all restricted key sets, with a log maintained of all key draws authorized to others on restricted keys. Sgt. XXX is implementing a color chit system, which will help address this issue.

Perimeter Security

- 18.01** There is written department policy that designates a security level to the institution and specific perimeter design/construction requirements related to that security level.

Observation:

No policy could be found that designated specific perimeter design/construction requirements.

Recommendation:

Because this institution houses inmates at multiple levels of custody, specific guidelines should be maintained for a minimum level of perimeter design, including double fencing, razor wire attachments to gates, and adjoining fences and lockdown features on electric gates.

-
- 18.02** There is written institution policy that establishes a requirement and procedures for continuous surveillance of the institution perimeter.

Observation:

No written policy requires continuous surveillance of the perimeter.

Recommendation:

Whenever possible, a 24-hour moving patrol should be implemented along with a vindicator mapping system for sufficient surveillance of the perimeter and rapid response to zone of alarm. Policy should describe the specific method by which continuous surveillance is maintained.

AUDIT INSTRUMENT REPORT EXAMPLE (CONTINUED)

- I8.03** There is an electronics technician on staff or on call who is formally trained in the maintenance and repair of all perimeter electronic detection systems and other electronic equipment in use in the institution.

Observation:

There are personnel who can be called in at all times to repair systems for perimeter detection, but certain staff voiced concerns that insects (spiders) could cause system to malfunction.

Recommendation:

More routine visual checks of equipment should eliminate this problem.

- I8.04** The number of inner and outer razor rolls and the type of barb used (long or short) are appropriate for the perimeter security category of the institution being reviewed.

Observation:

The number of inner and outer razor rolls was inconsistent along several areas of the fence. Double fencing was available in some zones but not in most. Ground razor wire was along the inner fence in some areas and should be at the inside bottom of the entire outer perimeter fence.

Recommendation:

The team recommends that facility security fencing be reviewed and a decision made concerning the minimum level and configuration of perimeter fencing acceptable and that the entire perimeter be upgraded to this level and configuration.

- I8.05** Perimeter lighting between the fences and thirty (30) feet on either side provides low-light vision and complies with department standards.

Observation:

Perimeter lighting was sufficient in most areas and provided good low-light visibility. Two areas inside the institution were considered to be problematic: Pine Bluff unit and the back of the horticulture area.

Recommendation:

Provide lighting in area adjacent to horticulture building for added visibility and at the front of the Pine Bluff dorm adjacent to HVAC systems. Remove or relocate the wooden shed in back of the horticulture area—blocks visibility and light.

Tabular Instrument:

The tabular instrument is arranged in a table format that provides information and space for recording information (see Attachment 2). Similar to the narrative instrument, the information is organized according to basic security topics (e.g., searches, visitation, key control).

Normally each row in the table addresses a specific standard. It is common for one instrument to contain several hundred standards. The standards should be officially accepted by the jurisdiction and are referenced in security policy. This feature ties the instrument and audit activity to the larger system of agency activity related to security program operation. Some instruments may only state the security standard; others cite the specific agency policy that describes the standard. For efficiency's sake, other instruments assume that all standards described are correct expressions and interpretations of agency policy.

ATTACHMENT 2

TABULAR SECURITY AUDIT INSTRUMENT

Function	AR 300-8 Key/Lock Control				
Authority	Authority Requirement	EX	C	EC	NC
SEC.III.N.3	The following areas have access by Restricted Keys:				
SEC.III.N.3.a	• Property storage		X		
SEC.III.N.3.b	• Evidence storage		X		
SEC.III.N.3.c	• Armory		X		
SEC.III.N.3.d	• Medical department		X		
SEC.III.N.3.e	• Primary issue point for keys		X		
SEC.III.N.3.f	• Administrative offices		X		
SEC.III.N.3.g	• Perimeter fence gates		X		
SEC.III.N.3.h	• Other critical areas as designated by the Administrative Head of the facility		X		
	• Check and observe restricted keys.			X	
	• Are all categories listed treated as restricted keys?			X	
	• Review restricted key signout log; compare to key box.			X	
SEC.V.A.1	From the Primary Issue Point, the Key Control Officer shall issue essential keyrings to secondary issue points. Secondary issue points shall be determined by the Administrative Head of the facility.			X	
	• Are these points identified in written policy and procedure?				

Each row contains space for recording information related to each standard, including a checklist and a space for auditor comments. These spaces are intended to allow the auditors to record their observations and conclusions with respect to each standard. Some of the checklist options are as follows:

Check “C” for Compliant: Systems operation and staff performance comply with the standard.

Check “NC” for Non-Compliant: Systems operation and staff performance do not comply with the standard.

Check “EC” for Essentially Compliant: Systems operation and staff performance nearly comply with the standard, but a few adjustments must be made to achieve full compliance. This designation should never be given without providing some direction in the comments section that *describes the adjustments to be made to achieve full compliance.*

Check “E” for Exception: Occasionally a standard may not apply to a facility being audited. For example, standards related to noncontact visitation may have no application to minimum or community custody facilities. As with the EC designation, this designation should never be given without some explanation from the auditor.

A comments section allows the auditor to record observations related to the nature of deficiencies and information for improving security practices.

The tabular instrument has several advantages:

- It allows for the collection and coordination of a large amount of security information.
- It can be quite complete, covering most or all of the security performance standards of the agency.
- Given that it is produced through a database or table management software, the information can be converted into different kinds of reports using the same information base, such as a simplified action plan for facility response or an executive summary focusing on noncompliant, compliant, and exemplary practices. The conversion may easily reduce a 30- to 40-page document to a very brief action plan of just a few pages.
- It has the potential to relate policy to standards and standards to sound conclusions based on observed practices.

The disadvantages of the tabular instrument include the following:

- It can be so extensive and detailed that it is a constant temptation for the auditor to be absorbed in its use and spend less time observing the quality of security practices. As a result, the audit takes on the character of a “paper audit” rather than one more concerned with actual staff performance.
- Complicated versions become very staff intensive, absorbing critical resources in trying to produce and understand reports.

- Should the instrument be “scored,” it may cause the organization to be more concerned with point totals than security practices.

The agency’s choice of format and content of the audit report should fit the needs and resources of the agency and should be user friendly to the people it serves. The design of the instrument is important for the reasons discussed above. However, it is more important that the agency initiate and promote a professional audit program and not be delayed or hindered by difficulties related to format and content. Most audit instruments include some or all of the following:

- Audit information page(s) with space for the name of the facility being audited, date of audit, and names of the auditors.
- Instructions for use of the instrument as a self-audit tool (optional).
- A table of contents that lists the security categories contained in the instrument.
- Points to be reviewed (security standards and expectations) by category.
- Columns for indicating compliance/noncompliance, yes/no, or another indicator of the auditor’s findings.
- Space for additional categories as may be needed (for example, a specialized program facility may have special security needs).
- Space for auditor comments.

The audit instrument, whatever its design, may include some, if not all, of the following categories:

- Armory/arsenal.
- Communications.
- Contraband/evidence management.
- Inmate counts.
- Control center operations.
- Controlled movement.
- Emergency plan.
- Fire safety.
- Food service.
- Hazardous materials management.
- Health services.
- Inmate mail.
- Inmate housing.
- Inmate transportation.
- Inmate visiting.

- Inmate work assignments.
- Key control.
- Perimeter security.
- Physical plant.
- Post orders.
- Release and discharge.
- Safety and sanitation.
- Searches.
- Segregation and special housing.
- Tool control.

Developing written security operations standards and an audit instrument can be exhausting. Many agencies have developed standards and instruments that other agencies may adapt to their own use. This document contains an audit instrument designed for that purpose.

Carefully developed policies, standards, and instruments are the underpinnings of a sound security audit program. They provide the authority, intent, direction, units of measure, and measurement tool. Without them, the audit can be less than credible, lacking in official sanction, and random (as opposed to planned, methodical, and comprehensive) in both process and outcomes.

In summary, few activities are more important than monitoring the security practices on which the health, safety, and security of staff, inmates, and the community depend.

It is through monitoring that risk and vulnerability are identified. It is through monitoring that poor/dangerous performance is identified and best practices highlighted. It is through monitoring that managers mentor and build the managers of tomorrow: Staff will *respect* what managers *inspect*.

The Security Audit Team

Audit Team Selection

Selecting the audit team members is critical to the success of a security audit program. Audit team members should be the most experienced and security-capable staff in the agency. Experienced security staff can learn *auditing* on the job; auditors who lack sound security experience cannot learn *security operations* through on-the-job auditing.

Experienced security staff can learn *auditing* on the job; auditors who lack sound security experience cannot learn *security operations* through on-the-job auditing.

Criteria for selection of auditors should include the following:

- Extensive security knowledge and experience at the manager/supervisor level.
- Understanding of line-level security practices and expectations (familiarity with post orders).
- Knowledge and comprehension (the “whys”) of department policies and procedures.
- Sensitivity to health and safety requirements.
- Good interpersonal skills and relationships; general acceptance as a credible security practitioner.

A security audit is much more than administering a questionnaire. It is not possible to develop an audit instrument that is so all-inclusive that reviewing only the issues in the instrument will provide a comprehensive audit. Auditors must be equipped by their security experience to assess risk and vulnerability as they audit a facility’s compliance with standards, policies, procedures, post orders, etc., and as they observe how those requirements are met. While a standard or expectation may be fully met, how it is met may create more risk or vulnerability than if it were unmet. Only experienced security practitioners have the capacity and ability to conduct risk assessment at this critical level. Detecting “what is” is important; awareness of “what could be” or “what could happen” is essential.

Audit Team Training

Team members must receive training not only in auditing protocol and successfully accomplishing the audit, but also in the interpersonal aspects of conducting an audit. Awareness and sensitivity to staff concerns and fears, techniques for avoiding confrontation, and eliciting the support and assistance of the facility being audited should be stressed in each training activity with auditors.

The following are suggested considerations in the training of auditors:

- Develop at least a 4- to 8-hour training session for potential auditors.
- Deliver training to staff *before* auditing begins.
- Provide initial training and frequently update the knowledge and comprehension of department policy, standards, and regulations as changes occur.
- Provide initial training in knowledge and understanding of the audit instrument and its application.
- Provide initial training, postaudit debriefings, and annual updates on audit technique and protocol: the *how to’s* and the *should not’s*.
- Accredit the training course so that staff receive credit for participation.

Chapter 2 discusses a key element of auditor training, technique. It cannot be overemphasized that the validity and effectiveness of a security audit will be in direct proportion to the knowledge and skill of the auditors.

CHAPTER II.

HOW TO PERFORM A SECURITY AUDIT

Functions of a Security Audit

A primary function of a security audit is to identify areas of vulnerability and thereby enhance the safety and security of staff. Done well, however, the audit has other very significant benefits. The greatest of these is providing a forum for teaching sound security practice and for learning from the work and experience of others. This being the case, the audit should be viewed as a welcome and helpful process. Unfortunately, institution staff most often perceive an audit to be a negative experience.

In most instances, the reason for this perception is that audits have been conducted in a confrontational manner (or are viewed as confrontational) and tend to mobilize the defensiveness of those whose area of responsibility is being audited. In the experience of many staff, “negative” audit findings have resulted in embarrassment, caustic reprimand, and even discipline. When staff perceive the security audit as an “I gotcha” exercise, an effort to catch staff doing wrong, rather than a tool to enhance safety and security, they will react defensively. This can be a difficult perception to overcome. It is critical that steps be taken to develop a security audit program that conveys a nonconfrontational, helpful perspective.

When staff perceive the security audit program as an “I gotcha” exercise, an effort to catch staff doing wrong, rather than a tool to enhance safety and security, they will react defensively.

Once weaknesses or deficiencies are identified, the institution manager should be required to develop a plan to address the problems identified. Training, modified post orders, new equipment, changed procedures, or a host of other remedies can be developed. *Discipline of staff should NOT be one of them.* Auditing is for the purpose of learning and improvement; supervision is for the monitoring and correcting of staff. If discipline becomes necessary, it should grow out of the supervisory relationship.

A second reason for security audits being viewed as negative or meaningless is the failure to use credible auditors. As indicated the section, “Audit Team Selection,” in Chapter I, credibility of auditors is critical to the success of the audit program. When staff view auditors with a “what do they know about it” attitude, they may ignore the auditors’ findings.

Staff should be reminded of the seriousness of their responsibilities. Complacency and routine are the enemies of sound correctional practice. Deficiencies *must* be identified and corrected; risk and vulnerability *must* be recognized and diminished. Staff should be reminded that the safety and security of the working/living environment is everyone’s responsibility and in everyone’s best interest.

Understanding the Security Audit

The security audit process is not just a “paper process” composed of checklists. It requires the auditor’s full attention and application of all his/her skills as well as an understanding of the correctional imperatives and the correctional environment. The auditor must be objective, experienced, openminded, flexible, willing to listen, and alert to the positives and best practices observed as well as pointing out deficiencies.

A correctional institution is a complex environment with an ebb and flow of control and privilege, which is largely monitored in the relationship of the keeper and the kept. Much of what “goes wrong” in the security operation develops in that complex relationship. The auditors must understand that “ebb and flow” of the institution and delve into what happens on a day-to-day basis in the interactions among staff, inmates, and others.

Correctional practice and processes will vary between institutions based on differences in mission, staffing, offender population, security and custody level of the institution, types of programs offered, and the physical plant. These differences require variance in security operations from one institution to another, while agency security *standards* prevail in both. As auditors move from one institution to another, they must have the understanding and capacity to incorporate the variances into their thinking as they assess the operations.

A “fresh eyes” approach is an absolute necessity in conducting a comprehensive audit. Staff often become complacent with established routines and mundane tasks. Shortcuts abound, and some new staff may have never been taught proper procedure. Supervisors are not immune to such complacency, and they too can “walk past” and not notice breaches or violations in security. *Fresh eyes* specifically focused on security and a new perspective will identify many issues and situations where staff have created shortcuts, abandoned essential security practices, or simply become complacent in the routine of the day. Auditors should not shrink from the responsibility of identifying risk or vulnerability that may exist, irrespective of the reasons for its existence.

A correctional institution is a complex environment with an ebb and flow of control and privilege, which is largely monitored in the relationship of the keeper and the kept. Much of what “goes wrong” in the security operation develops in that complex relationship.

Preparation for the Audit

Preparations for an audit should reflect the seriousness of the auditing responsibility.

The auditors must be well grounded in the agency's security operations standards. These are the basis of the audit, and all operations must be assessed in light of these standards. If the standards are unclear or contradictory, this must be addressed in writing, so that all auditors and institution managers share the same understanding. For example, a standard that says "periodic security checks must be made" will be interpreted in many ways—15, 30, 45 minutes—and is not a measurable standard. It will be helpful to define "periodic" if disputes of interpretation are to be avoided.

The auditors must also be so familiar with the security audit instrument that they do not need to rely on the written document during the audit. It cannot contain all the points of review relevant to every institution and every situation. The audit instrument should identify critical points of review, but the auditors will observe many issues that the audit instrument does not mention, each issue leading to another until the points and scope of risk or vulnerability are exposed. The security experience and knowledge of the auditor will provide the insights and understanding that will guide him/her in a productive direction as questionable issues are observed. Lack of familiarity with the instrument and with sound security practice will cause the auditor to be tied to the instrument, and the result is likely to be a "paper audit."

The security experience and knowledge of the auditor will provide the insights and understanding that will guide him/her in a productive direction as questionable issues are observed.

It is recommended that each institution be required to prepare a packet for auditors that contains, at a minimum, the following information:

- Institution mission.
- Organizational chart with names through firstline supervisors.
- Current footprint of the institution.
- Program description.
- Inmate profile.
- Special issues or problems of which auditors should be aware or to which the warden would like them to give attention.

This information will enable the auditor to achieve a greater level of comfort as the audit begins.

Security Audit Technique and Protocol

Audit Technique

Adopting a technique or method for the security audit makes the task easier. And though security auditing is not an exact science, technique is involved that makes a complex task less complex and ensures that the audit will be comprehensive. The training of auditors should include extensive discussion of audit technique and protocol.

It has been said that a comprehensive assessment/audit must include four elements:

- What is written? **READ**
- What is said? **LISTEN**
- What is done? **QUESTION**
- What is done? **OBSERVE**

This is the heart of auditing technique. All four elements are important in achieving a valid outcome. They provide checks and balances and enable the auditor to get as near to actual practice as is possible, given the time limitations and the magnitude of the task.

READ:

Are policies and procedures complete, up to date, and accessible to those who need to know?

Are policies, procedures, and post orders clearly written and in user-friendly format?

Do post orders and policies conflict? If staff are aware of the conflict, a situation of stress/tension exists and performance will suffer.

Do posted notes, memos, and orders at officer stations and elsewhere countermand policy, procedures, or post orders? Is the writer a duly appointed authority?

Are logs, forms, inventories, and other documents that staff must fill out legible, complete, current, and in compliance with requirements as stated in policy, procedure, or post order? (Review both current and past logs, inventories, reports, etc.)

LISTEN:

Actively listen to staff—not only in response to your questions but to what they want to tell you. Inmates may wish to discuss issues as well. These discussions can provide an auditor with insight into the tone and climate of the facility.

Hear staff comments about “audits”; it will help you understand their perspectives and attitudes and in forming your approach as you do your work.

Listen to what staff are *not* telling you. They may be reluctant to tell you outright that they rarely see a supervisor or administrator at his/her post but you can “hear” that message in other ways.

Hear words, tone, and expressions that suggest fear, anger, pride, complacency, and boredom.

QUESTION:

What is the facility/staff experience with audits? Do they perceive audits as a “gotcha” exercise? Are they likely to be helpful or to hide what they can? Awareness of staff attitudes can help the audit team determine how to approach the audit.

Do staff have recommendations for enhancement or improvement of a specific aspect of operations? They will sometimes share ideas without being asked but, by asking, the auditor can involve them and elicit information about concerns they may have about their post. Suggestions by staff should be noted as a positive contribution (with the staff member’s name) during the debriefing session and in the final written report. Doing so will help build staff confidence and trust in the audit process.

Conduct verbal on-post testing. For example, does the staff member understand his/her responsibility and/or proper response to a specific type of emergency? This is sometimes referred to as the “what if” exercise.

Conduct on-post proficiency tests. Does the staff member know how to operate a specific piece of equipment safely?

Does the staff member understand the post orders for his/her specific area of responsibility?

OBSERVE:

Don’t rely only on written policy/documentation; review practice. The written word tells only a fraction of the story in security assessments. Does practice conform to policy, procedures, and post orders? *Are we doing what we say we are?*

Observe operations. Note the degree to which practice conforms to policy requirements, post orders, and other written instructions. Observe staff searching a vehicle, inmate skin and frisk searches, visitor access to the facility, and the use of metal detectors and other technology.

Coordinate observation during formal counts or other institution activities. Separate the team to observe various aspects of the count or other activity.

Test security systems. For example, test the key control system by having a staff member take you from outside to a specific point inside the facility, perhaps using emergency keys. Inform staff that you are conducting the test, state the purpose of test, and explain that the tests are meant to be learning opportunities.

Complete at least one systems check during the audit.

Assessing the Environment

Though points to be reviewed are defined in the audit instrument and suggested in standards, policy, procedures, and post orders, the institution environment should also be assessed. The institution environment in which staff work and inmates live is important. If it is positive and

healthful, it promotes growth and actualization. If it is negative, it will be demoralizing and destructive. Although there are few “hard” issues to audit, auditors can observe many indicators that will give them a sense of the environment.

Once again, solid security experience comes into play; with experience comes an ability to “feel” or “read” the prison environment and to identify aspects of the facility and operation that suggest negativity. Among the aspects of the facility and operation that the auditor must review are the following:

Sanitation: Are good sanitation practices enforced *throughout* the facility? A lack of acceptable sanitation can frequently indicate serious management and supervision issues within a facility. Do sanitation practices create an environment conducive to inmate pride and positive staff morale while providing opportunities for inmate jobs? Are there waste, clutter, facility deterioration, and unclean conditions that may create a fire, health, safety, or security hazard?

Facility Tone and Climate: What is the inmates’ frame of mind? What type of complaints do they have? Is the general feeling within the facility positive? Do inmates make eye contact with staff? What are the nature, frequency, and tone of grievances? Are grievances taken seriously? Are staff comfortable and confident in confronting and correcting inmates in order to enforce institutional rules and other requirements?

Staff Morale: Are staff positive and upbeat? Do they take pride in their work? Are they generally cooperative with auditors or reluctant to speak up? In the latter situation, auditors should consider the reason for reluctance and lack of cooperation; it may be because of punitive supervision or leadership or generally low morale. If this attitude is pervasive, it should be noted in the audit report. When staff morale is low, staff are not in tune with the institution’s mission, and security will suffer and complacency will become commonplace.

The Auditor’s Role

The “Good Neighbor” Auditor

Auditors sometimes have difficulty understanding their role and the limits of their responsibility. Put in a position to observe, question, and report deficient practices, there is often a temptation to feel a sense of “power” in the position. In a correctly designed audit program, the auditor role has NO position power.

The role of the auditor is to *identify* and *report* (to designated leaders) conditions that in the auditor’s opinion are in variance with agency policy and standards and, in

Proper understanding of his/her role provides the auditor freedom to identify areas in which improvements could/should be made without being limited by factors that impinge on the situation (e.g., cost, staffing, labor agreements, facility limitations).

most agencies, *recommend a more appropriate condition. All decisions concerning the report and recommendations are then in the hands of decisionmakers.*

As the role is properly understood, auditors come to be viewed by staff as vehicles for communicating ideas, needs, and workplace frustrations to the leadership of the organization. These ideas should be passed on, perhaps as part of a recommendation, and the staff given credit by name for the idea or practice. Proper understanding of his/her role provides the auditor freedom to identify areas in which improvements could/should be made without having to consider all of the factors that impinge on that situation (e.g., cost, staffing, labor agreements, facility limitations). In so doing, the auditor “pushes the envelope” and encourages consideration of options that may have previously been ignored or denied because of the known limitations. If the situation/condition poses a potential risk or vulnerability, it should be reported irrespective of such factors. The decisionmakers then have responsibility to determine what is to be done, if anything, to correct the deficiency.

Auditor-Staff Relationships

When entering an area, audit team members must *always* be introduced to staff and the purpose of their presence in the facility explained. Remind staff that the purpose of the audit is to review operations and identify ways in which safety, security, efficiency, and effectiveness can be improved. Ask for their input: “What could be done to make your post more efficient and effective?” Do your best to put staff at ease.

When questioning staff, it is important that the audit team be sensitive to the fact that a staff member may be feeling pressured and in a difficult spot. If a staff member seems reluctant to answer, do not push him/her to respond, Move on to another question or to another staff member. Never be critical. Ask questions or discuss; engage staff in conversation.

Avoid comments such as “*You need to...*” “*You must...*” or “*You should...*” Such comments are often felt to be condescending and are beyond the scope of responsibility or authority of the auditor or audit team. Comments about how “*we do it*” should be offered only in a discussion in which the staff clearly wish to compare practices or ask for ideas on how they could change their operation. Even then, they should be reminded that any change would have to be authorized by their warden or superintendent.

It is important that auditors not record confusing, purely speculative observations that have little constructive value to users of the audit results. Should the auditor’s comment be a recommendation for improvement that is not required by policy, he/she should be clear on that issue.

Do not enter into arguments about your observation. Accept explanations of why the condition is as it is and make note of it, but *do not* become judgmental or argue about whether the condition should be as it is. The auditor’s role is to report the condition; it is the responsibility of the decisionmakers to determine it if should be changed.

Having outsiders looking over one's shoulder will always be a source of some discomfort to those being audited. Although such reactions are not fully in the auditor's control, conducting the audit in a positive manner will relieve much of that discomfort and will contribute greatly to the likelihood of an outcome that makes the institution more secure.

Scheduling Audits

For the first year or two, security audits should be scheduled in advance to enable the institution managers to get accustomed to the idea, avoid scheduling conflicts, and create minimal interference with institution operations. When defensive attitudes and perspectives concerning security audits prevail, advance scheduling is critical. Such attitudes and perspectives will only change over time as staff come to trust that audits are not being conducted as a means of *getting staff*, *catching* the institution in a situation of noncompliance, or *punishing* a facility or staff for problems it has had. If the department of corrections has gained a "gotcha" reputation, deserved or not, in its supervision and oversight of individual correctional facilities, it will take time to develop a positive staff response to the audit process. Clearly announced audits—well in advance of the scheduled date—will go far in alleviating such fears.

It is generally believed that security audits should be conducted at least once each year at each institution. In a large agency, this is a large commitment of time and resources. Some have interchanged *self-audits* and *formal external audits* because of limited resources. If this approach is taken, it is recommended that the audit program begin with the formal external audit to establish expectations. Self-audits should be reviewed by a central security manager with followup and assistance in addressing deficiencies. Audits without actions to rectify deficiencies accomplish nothing and establish or reinforce a *laissez-faire* institution climate.

Audit duration is generally determined by the facility size, security and custody level, and complexity of operations. Security audits will typically require a full week, but duration may vary based on the above factors, the number and experience of the auditors, and whether there are special issues that must be reviewed.

The presence of auditors in the facility during evening/night hours should be required for the purpose of evaluation of perimeter lighting, observation of housing areas when fully occupied, and opportunity to talk with staff on these shifts and allow them to contribute to the audit. A "real-world" view of the institution must include observation during the hours in which there are fewer program, supervisory, and administrative staff present.

Following the development of an audit program, it is common for a warden to request an interim audit, sometimes a "surprise" audit. This generally indicates that the program is succeeding and the process is being viewed as nonthreatening and helpful. Such requests should be accommodated, but audit staff should be mindful that the warden's acceptance of the audit process might not reflect the feeling/attitude of all facility staff. Such audits should be conducted with as much care as initial or annual audits.

When the audit process has been incorporated into the department's policy and routine operations (usually after about 2 years), audits can be conducted on a random, unscheduled basis, if that is the direction the department chooses to follow. Through a combination of scheduled and unscheduled (surprise) audits, a department can achieve maximum efficiency and effectiveness in its audit program.

Resources Needed

Properly equipping the audit team will contribute to its efficiency, its effectiveness, and the perception of its competence and preparedness. At a minimum, each auditor should be equipped with the following at the time of each audit:

- Notebook containing the following resources:
 - Audit policy.
 - Current agency security operations standards.
 - Security audit instrument.
 - Notebook paper.
 - Institution familiarization packet.
 - Incidental materials.
 - Highlighters, pens, pencils.
 - Clipboard.
- Attire
 - Professional, but comfortable clothing (females may want to consider not wearing dresses or skirts when auditing, as climbing stairs, towers, and steps may be part of the process),
 - Comfortable footwear (lots of walking, climbing).
- Computer/laptop.

Some agencies have equipped auditors with laptop computers. This equipment facilitates the compiling of information and development of an audit report. Initially, however, a department may wish to allow auditors to develop their skills free of the necessity of inputting information from notes taken during the "walkaround" process and provide computers as they become more comfortable with the audit process.

Audit Team Site Preparation

To accomplish its work, the audit team will need the following accommodations and resources, some of which may have been provided in the preparation packet recommended:

- Designated, private conference/office space to work in for the duration of the audit.
- Computer availability in the work area.

- Telephone access.
- Facility schematics and map.
- Inmate handbooks and program descriptions.
- Institution policies/procedures.
- Facility post orders.

The audit team may also request that a staff member be available to escort team members to specific areas, contact staff with whom they need to discuss issues or practices, and assure that other team needs are met. The staff assigned can also provide necessary documentation as the audit team may request.

The credibility of the audit process and the validity of the concerns noted by the auditors are enhanced when a staff member from the audited institution accompanies the auditors and “sees what they see” to better understand the justification for any findings reported.

Preaudit Briefing

The audit team should schedule a preaudit briefing with the warden and key staff identified by the warden. The preaudit briefing should consist of:

- Introduction of audit team members.
- Introduction of facility staff.
- Overview of the audit process.
- Tentative time schedule.
- Discussion of special concerns the warden and/or staff may have concerning the audit process or conditions in the institution.
- Opportunity for the warden to request special attention by the audit team to a specific area or problem.

It is important that an appointment for a postaudit, verbal debriefing be made at this time. The warden may request and should be given the opportunity to receive a daily debriefing. Other staff may be included in this debriefing as determined by the warden.

Preaudit Tour

The audit team should tour the facility before commencing the audit if the entire team is not familiar with the facility and its programs, architecture, etc. This tour can be conducted on the morning of the first day of the audit. The tour should be short but provide exposure to all areas (e.g., industries, housing areas, education, programs, special housing areas), although the team should not necessarily visit every housing unit or the gymnasium, classrooms, laundry, and other nondescript areas. The audit does not start during this tour; rather, the team is getting the “lay of the land” and

a general sense of the condition of the facility. There may be opportunities to ask questions, but they should be limited and attention should be on getting an overview of the facility and its operation. Obvious security-related deficiencies should be noted with a plan to explore further after the tour is completed.

As indicated above, the role of the auditor is “to *identify* and *report* (to designated leaders) conditions that in the auditor’s opinion are in variance with agency policy and standards and, in most agencies, *recommend* a more appropriate condition. Experienced auditors will also observe conditions, practices, situations, or problems that are not at odds with policy and standards but that they know could be improved. These should be pointed out—offering helpful suggestions for improvement of the operation.

Security System Checks

The auditor’s role and the techniques used in conducting an audit have been discussed. An important final technique, both in auditing and in ongoing monitoring of the institution operations, is the security system check. A security system check is a simulated emergency designed to test the adequacy of emergency plans and to test staff knowledge, practice, response, and equipment in various situations. To test staff knowledge, practice, response, and equipment only in time of actual emergency is courting disaster.

To test staff knowledge, practice, response, and equipment only in time of actual emergency is courting disaster.

The purpose of security system checks is, as in other audit activities, to identify areas of risk and vulnerability. Their purpose is not to trick staff; rather, it is to determine areas where additional training may be required, post orders modified or clarified, procedures changed to address changing conditions, equipment upgraded, or supervision strengthened.

A security system check may be as simple as asking a perimeter staff officer, “What would you do if...?” or “What weapon would you use if...?” and “What is the effective range of that weapon?” Another type of check might be, to determine if the visiting room is searched after a visit, leave in the room an envelope with a note in it that directs: “When you find this note, return it immediately to the Captain.” Similarly, a card with a similar directive can be affixed to the perimeter fence to determine if those checking the perimeter are paying attention to the fence and its condition. Testing responses and response times to perimeter intrusion alarms, exchanging IDs and attempting to enter the facility, “planting” a note in a transport vehicle, and other challenges to the security systems can be used to check the system.

A program of security system checks should be announced beforehand, and an example or two provided so that staff know what to expect. The purpose of the program should be clearly announced and staff informed that discipline will *not* follow staff “failure” of a test. Rather, steps will be taken to improve performance in the future, be that by training, guidance, mentoring, or other types of assistance.

Security system checks should never expose staff or inmates to risk or harm or injury or jeopardize institutional security. They should be thought through and authorized by institution administration. Supervisors should be encouraged to discuss duties with staff on post and question them concerning their knowledge and skills. In authorizing security system checks, the following should be considered:

- What is being tested?
- Who should participate?
- Who should have advance notice of the test?
- What safeguards should be in place?
- What specific instructions should be given to the participants?
- How long will the check continue before termination (if applicable)?
- How will the debriefing be handled?

Following a system check, a debriefing should *always* be held with staff involved. Including the institution's training supervisor reinforces the administration's interest in increasing the effectiveness of the training. The employee's supervisors should be present, and members of the administrative team should participate whenever possible.

Security system checks can be a valuable learning tool, both as part of the audit program and as an ongoing monitoring program. Their judicious use is encouraged to improve staff performance, reduce the routine and boredom inherent in some post assignments, and address the complacency that invariably creeps into the security operation.

CHAPTER III.

THE AUDIT REPORT

For security systems to reach higher performance levels, the recommendations for improvement and standards compliance in the audit report must be converted from information to action. Until this occurs, the resources expended in conducting a quality security audit will not have been used to their full potential, and the audit report may “gather dust on an office shelf.”

The report must be treated as an essential ingredient in the correctional organization’s strategic plan to elevate the quality of security systems and practices to the highest level possible. For that to happen, the design of the report must be consistent with the style and needs of the management to be served, and the report should be a part of a larger agency emphasis on security performance. For the audit report’s findings to be translated into improved safety and security, it is essential that point-by-point corrective action be taken in response to the recommendations.

For the audit report’s findings to be translated into improved safety and security, it is essential that point-by-point corrective action be taken in response to the recommendations.

Components of the Audit Report

The security audit report presents the combined results of four activities: emergency findings, daily briefings, the audit outbriefing, and the formal written report.

Emergency Findings

The emergency findings consist of observations that raise an immediate concern for the safe and orderly operation of the correctional institution. In the NIC *Conducting Security Audits* seminar, these are referred to as “Oh my god!” issues—issues that must be immediately reported to the leadership of the facility for resolution because of the serious risk or vulnerability they represent. Such observations may not become a part of the security audit report—such an incident may be purely idiosyncratic. Nonetheless, followup is essential to ensure that the underlying problems have been addressed.

Daily Briefings

During the audit process, the audit team should make itself available to the warden and staff. Many wardens appreciate a daily briefing on audit progress and may correct many deficiencies before the audit team leaves the institution. Priority attention should be given to any special requests made by the warden, and the findings and recommendations related to that request should be relayed at

the first opportunity. Daily briefings are helpful to the team as well, enabling them to observe the warden/staff's response to the findings and providing insights that may be helpful in delivering the final reports—verbal and written.

Postaudit Briefing with Warden

The outbriefing is normally held on the final day of the audit and reports on the most important findings of the audit team. The primary deficiencies should be clearly identified in a manner that would allow the institution's top managers to move forward with remedies, should they choose to do so, before they receive the written report. Because institutions are often anxious to move forward with improvements, delivery of the written report should be a priority of the audit team, and the audited institution should receive the report shortly after the conclusion of the audit. Especially for new audit programs, it is recommended that the agency's chief of security operations or other central office prison administrator be present for the debriefing. His/her presence will reinforce agency commitment to the process and underscore the audit team's authority in delivering its findings. It will also provide important feedback to the audit team concerning its performance, manner, and the degree to which its report is consistent with agency expectations. It is important that auditors understand early in the audit program their role and relationship with the institution managers. A central office administrator can assist them in finding a proper balance of assertiveness and aggressiveness.

The audit team should decide in advance which team member will report on what audit area and plan and rehearse the verbal report to the extent possible. This is especially important in a new audit program and for new auditors. The acceptance of the findings can depend on the manner in which the information is delivered. Practice makes perfect.

In delivering the report, avoid such phrases as “*you need to...*” and “*you must...*”. As said earlier, that is beyond the role of the auditor—the warden or central office administrator will decide if changes will follow the audit recommendation. Rather, the auditor should phrase recommendations as “*the audit team recommends*” or “*the audit team suggests*.” Avoiding first person representation—“*I suggest...*”—eliminates acceptance or rejection of the idea based on personality and correctly represents the audit as a team activity and an extension of agency authority.

When giving the verbal report, be kind but honest. Do not “gild the lily.”

Ideally, the audit report will have identified some “best practices” and other positive aspects of operations. Staff will have suggested ways in which the operation or their post can be strengthened. These should be mentioned in the report, crediting responsible staff by name. A balance of positive findings with deficiencies will help gain acceptance of the recommendations.

Time should be allowed for questions and comments from staff but argumentative discussion should be avoided. The report consists of auditors' observations and recommendations—

no decision has been made as to their acceptance. Auditors may provide a rationale for their position but should not enter into argumentative discussion of the merits of the existing conditions.

When giving the verbal report, be kind but honest. Do not “gild the lily.” Do not be *redundant* in praise to balance things that are difficult to say. It will be viewed as phony—rightly so.

The Written Report

The audit report format will ordinarily be determined by the format of the security audit instrument used by the agency. The report format design, in addition to including specific findings relative to security operations, should also include space for general comments concerning topics such as the general atmosphere of the facility, sanitation, staff morale, the mood of the inmate population, and the overall quality of the organization.

Narrative Instrument

When a narrative instrument is used, the report will consist of a narrative listing of observations and recommendations for each/most of the deficiencies noted. Because the narrative format does not contain an exhaustive listing of points of review, other observations or issues will also be noted, often as *Special Issues* with a recommendation for each. These should, for ease of reference, follow an uninterrupted, numerical sequence from the beginning to the end of the report. This feature also helps eliminate confusion when the report is quite extensive, containing many observations and recommendations. This format is simple and straightforward (see Attachment 1). An advantage of this format is that when completed, the audit report contains only issues where risk and vulnerability have been identified. A report “by exception” format reduces report length and emphasizes the issues needing attention.

Tabular Instrument

When a tabular instrument is used, the audit report will normally be in the form of a chart or summary checklist (see Attachment 2). The report will normally indicate the level of compliance with standards (see the discussion of designation of compliance levels in the tabular instrument under “Security Audit Instrument” in chapter 1) for each of several hundred individual standards-related points of review. As in the narrative instrument, the information will be organized according to basic security topics (e.g., searches, visitation, key control). The tabular report tends to be quite long and may result in a checklist with little helpful information unless the auditors are highly skilled and knowledgeable in security matters and have experience working with this audit instrument, which demands great attention to specific detail.

Scoring and ranking are meaningless when related to security auditing. Having a security audit score or rank may be likened to the value of knowing the “average depth” of a river: one can drown in a river with an average depth of 6 inches.

Because the format of the audit report is largely driven by the security audit instrument, it is important that the agency managers carefully consider the outcome that will be most useful to them when they select or design a security audit instrument. Whatever the choice, it should be consistent with the resources of the agency, the skill of the auditors, and the needs of the institution it serves.

Audit “Scores” or “Rankings”

In our competitive environment, we have a natural tendency to “score” things. “How did we do?” is a normal question following an audit. A typical response is often in the number of deficiencies or areas of noncompliance found. In some instances, a score is tallied following each audit, and institutions are ranked according to their score.

Scoring and ranking are meaningless when related to security auditing. Having a security audit score or rank may be likened to the value of knowing the “average depth” of a river: one can drown in a river with an average depth of 6 inches.

Consider this example: The first-ranked institution—the one with the best overall score—has two deficiencies. The second-ranked institution has 10 deficiencies. The first institution’s deficiencies are in the area of Class A tools and pose a serious threat to the security of the institution and the physical well-being of staff and inmates. The second ranking institution’s 10 deficiencies are in the area of handling of inmate mail, property, and laundry, none being serious. Can it truly be said that the first institution is a “better” institution or had a better audit outcome than the second?

The writers of this document are unaware of any benefits in scoring and ranking. Several problems should be considered before authorizing the scoring or ranking of audit outcomes. Scoring and ranking tend to do the following:

- Undermine the stated purpose of a healthy audit program: to learn of risk and vulnerability and improve the safety and security of the facility. The focus invariably turns from substantive issues related to safety and security to that of numerical outcomes and competition.
- Reinforce fears that audits are to catch staff/institutions doing wrong and perhaps find cause to punish staff.
- Reinforce a culture of suspicion and resistance around audits.
- Lead to coverups and diminished cooperation with auditors.
- Lead to paybacks as staff audit each other’s institutions.
- Create an “earning” culture rather than a “learning” culture.

A “win–lose” audit culture is a culture in which there are no winners. It is almost certain to diminish the value of audits as staff focus on the score and rank rather than on discovery and correction, and it creates a downward spiral in audit effectiveness.

Executive Summaries

The full audit report delivered to the institution and central office at the conclusion of the site visit can be quite long. Many pages may simply report that the facility is compliant with specific standards. Executive staff are extremely busy people. Documents for them need to be reduced to the essence of important information in a user-friendly format.

It is suggested that the original report be reduced to include only reports of “noncompliance” and, if applicable, “essentially compliant,” and reports of compliance that refer to exemplary practices. In addition, it should include recommendations for improvement in practices that are not violations of policy standards.

The report derived from a narrative format instrument is essentially an executive summary that includes primarily those issues in which action is recommended for improvement. Care should be given to ensure that the issues are properly ordered, with a table of contents, clearly articulated, and a section added to each issue in which the warden can indicate his/her plan of action.

If systemwide action is recommended, issues from all institutions can be collapsed into a single report to reflect the overall agency status/need as related to a specific security topical area.

Report Distribution and Followup

Report distribution requirements vary among agencies. However, the auditors should normally deliver the full audit report, with executive summary if required, to the institution within 2 to 4 weeks following the conclusion of the audit. The institution should be expected to develop a complete action plan that addresses each area of deficiency within a reasonable time thereafter, submitting it with a copy of the audit report (or executive summary) to agency executive staff. The action plan should include information concerning the resources required to implement the audit recommendations and a timeline for each of the proposed changes or improvements.

If the institution disputes any of the findings, these are normally appealed to the chief of security operations for a final determination to be made.

A copy of the audit report (executive summary) and action plan is provided to the audit team at the time of the next audit.

Legislative/Gubernatorial Reporting

One of the best indicators of a quality organization and a proactive approach to success is that members have the same degree of commitment and a shared understanding of critical issues at all levels of the organization. In a correctional organization, few disagree that security is a critical issue. A proactive, forward-looking correctional security program should include an annual security report to key legislative agents and, in state agencies, the Governor’s office. It can become the basis

of uniting all players on important security issues. This type of report should be general in nature, outlining the security concerns and accomplishments of the performance year for the department of corrections (see Attachment 3 as an example). A separate budget line for security hardware, equipment, and systems can be a productive companion to this version of the audit report.

Confidentiality

The audit report is likely to indicate where security is not performing at its best and recommend improvements. Obviously, it could be damaging should it fall into the hands of inmates. Therefore, it should be used and stored in areas where inmates have no access under any circumstances. Additionally, the media or private interest groups may have a keen interest in the contents of the report. In some circumstances it may be an advantage to the department for them to know the content. However, it must be remembered that the media or private interest groups can become adversarial at any time and may use any part of the report to discredit the department or call its operations into question. The best policy is not to make audit reports available outside the correctional department except by court order or the discretion of the executive director.

One of the best indicators of a quality organization and a proactive approach to success is that members have the same degree of commitment and a shared understanding of critical issues at all levels of the organization.

Action Plans

As indicated earlier, the audit report should contain a comments/action plan section in which the warden can note the desired action. Where the audit report indicates a condition that does not comply with performance standards or a general condition that could be improved, the decision to act should be recorded as the action plan for that standard. Audit policy should direct that the action planning be a collaborative process by which facility staff consider possibilities and select strategies for achieving success. The results would list steps for implementation, persons responsible for each aspect, and expected completion dates.

Conclusion

The audit report should be designed to be compatible with a larger departmental effort to achieve the highest levels of security. The format should be efficient and user friendly and should provide enough information to be useful to the facility or organization to be served. It should be a modified version of the audit instrument that fully integrates the standards being audited, the conclusions of the auditor, helpful clarifications, and an action plan to improve security program operations. Under an umbrella of confidentiality, the report should be distributed and made available to key corrections and governmental staff that have a direct role in managing the organization.

DEPARTMENT OF CORRECTIONS SECURITY LEGISLATIVE REPORT

State statute requires the Director of the Department of Corrections to, at a minimum: conduct or cause to be conducted announced and unannounced comprehensive security audits of all state and private correctional facilities. In conducting the security audits, priority shall be given to older facilities, facilities that house a large proportion of violent offenders, and facilities that have experienced a history of escape or escape attempts. At a minimum, the audit shall include an evaluation of the physical plant, landscaping, fencing, security alarms, and perimeter lighting, and inmate classification and staffing policies. Each correctional facility shall be audited at least annually. The Director shall report the general survey findings to the Governor and the legislature.

To this end, the Director initiated an unannounced security audit process augmenting the security component of the existing management review process. An audit team comprised of individuals with extensive and diverse institutional security experience was formed to operate out of the Department's Bureau of Security Operations.

The process utilizes regional and facility personnel to conduct announced audits of half the Department's facilities annually. The unannounced audit team is responsible for conducting audits of the remaining facilities and adjoining units. Great care is taken to maintain the confidentiality of the selected audit locations and NO advanced notice is given. The wardens and facility staff are only advised of the audit following the arrival of the team. This facilitates a more accurate, realistic picture of the day-to-day security operations and provides for a better assessment to identify deficiencies and security needs. The first audit utilizing the new process was completed December 21, 1995. Since that time a total of 34 audits have been completed.

The audit instrument used by the audit team contains 238 standards, which were primarily derived from existing policy requirements. Facilities are required, at a minimum, to comply with these standards. The audit process also considers other areas not necessarily covered in the audit instrument relating to the security systems of individual facilities with unique mission requirements. The audit instrument is subject to revision and additions based on the identification of new areas of concern as well as best practices developed at specific institutions and noted for special mention. Deficiencies in the physical plant that might impact security are also reported.

Upon completion of an audit, a detailed report is submitted. This report lists the deficiencies discovered during the audit as well as recommendations for how they are to be corrected. This information is then shared via security advisories disseminated statewide to all facilities in an effort to ensure consistency and promote continued improvement of our security systems. Upon receipt of the audit report, wardens are required to submit a corrective action plan to the Director of Prisons within 30 days. Random unannounced followups are then conducted by the audit team to ensure the corrections listed in the action plan have taken place.

The written report should never depart significantly from the informal outbriefing provided to the warden and staff. When the written report is delivered, it should contain no major surprises. A security audit report, responsibly completed and delivered, can and should become a welcome “to do” list that, when completed, will add to the safety and security of the facility.

Although the report and followup activity are important outcomes, it is also important to recognize that much benefit is gained from the audit *process*. The attention to policies, procedures, standards, post orders, staff, operations, equipment, and facility all bring tremendous attention to the importance of sound security standards and practices. In addition, however, attention to a formal written report and the development of an agency-supported action plan, with resources provided where needed and when possible, are “frosting on the cake” and a powerful force in the ongoing development of safe and secure institution operations.

CHAPTER IV.

THE SECURITY AUDIT INSTRUMENT

How to Use the Security Audit Instrument

This security audit instrument has been used during the audit of numerous institutions that have hosted NIC *Conducting Prison Security Audits* training seminars. Refinements have been made based on the experience of the participants, the “best practices” of the facilities, and the recommendations of audit team leaders. Although it includes many of the essential elements of a sound security program, the instrument is not designed or intended to meet the final audit requirements of any agency or institution until it has been tailored to that agency or institution’s specific needs and requirements.

There is no “one size fits all” in the world of audit instruments. Existing instruments range from those that are policy based with little attention to practice to those that are fully based in the detail of security practices. Contents of audit instruments vary, reflecting differences in security standards and operations among correctional agencies and differences in what various institutions have decided to audit. However, there are many similarities in core security principles and practices. Recognizing this, this instrument was developed as a “model” that incorporates many/most of those essential elements and can serve as a foundation document that can be adapted to state and institution security policies, procedures, standards, and practices:

- One of the differences among correctional agencies is in **terminology**. The terms used in your audit instrument must reflect the common usage and understanding in your agency.
- Other differences are in written **policy** and whether there is written policy (by design or oversight). The security audit instrument is intended to suggest policy: that is, it asks about written policy in those areas in which most security specialists believe written policy should exist.
- Not only does “what” agencies require differ but “how” it is to be accomplished also varies. Thus, written **procedures** differ among agencies, and it is essential that the audit instrument be adapted to reflect the agency’s expectations.
- Agencies also vary in **standards**: the minimum level of performance or response to a policy, issue, or problem. Whether the standards are internal or external (statutory, American Correctional Association, or other), the adapted audit instrument should reflect them as points of review.
- **Practices** among agencies diverge significantly based on many factors, including the mission of the institution, staffing levels, available supervision, and physical plant. In adapting the instrument, such factors must be considered.

This audit instrument is a starting point for the development of a comprehensive audit instrument. Though some may choose to use it as is or with minor alterations, its best use will come through careful adaptation to more nearly incorporate each agency's security philosophy as reflected in its policies, procedures, standards, and practices.



ALL PERSONS PARTICIPATING IN THE SECURITY AUDIT PROCESS SHOULD READ THE FOLLOWING THOROUGHLY BEFORE PROCEEDING.

Before conducting an audit, whether using this instrument or a fully adapted version, each auditor should understand the following:

This security audit instrument, like all others, is not all inclusive. Many security details that are important to the security of an institution are not in this instrument.

The security audit instrument will direct the auditor to the areas where potential security lapses may occur. It is important that each auditor have extensive security experience that enables the auditor to recognize security weaknesses or deficiencies in the details of institution operations.

The task of the auditor(s) is factfinding: The warden, the institution's staff, and the warden's superiors determine the presence of error or the need for change. If the auditor cannot give a positive response at each point of review, it should *not* be inferred or suggested that the institution/agency is in error or that the security of the facility is in jeopardy; the auditor should simply state the observation. An institution/agency may have thoughtfully decided, for good reason, not to require by policy or in practice certain broadly held security practices. If such a decision seems to the auditor to create a potential risk situation, the auditor should note that with a recommendation that the institution/agency decision and practice be reviewed. Similarly, if written policies and/or procedures are lacking or inadequate, or if the state of staff knowledge and security practices suggest the potential for a breach of security, the audit process should clearly communicate this. *Critical deficiencies that, in the opinion of the auditor, could create an immediate risk to safety or security, should immediately be brought to the attention of institution managers.*

Auditors should recognize that institutions of differing security or custody ratings, program objectives, architectural structure, staffing complements, and inmate profiles may present different risk characteristics. An apparent deficiency in one institution may be more critical than in another. *However, security deficiencies should not be passed over because they seem to be less critical because of the custody level or other characteristics of the institution.* Those who are responsible for the security of the institution should identify and review all deficiencies.

A security audit that is not thorough, thoughtful, and conducted by credible persons can have the opposite impact of that intended:

- An audit that “glosses over” or fails to report security deficiencies may suggest to staff that the issues are not significant and give a false sense of security.
- If the audit is not done carefully and accurately, misleading findings or recommendations may be made and the audit report “discounted” or ignored.
- If the persons conducting the audit are not experienced and credible, the report and recommendations may not be viewed as credible.
- If an audit is conducted with a “gotcha” attitude, staff may be uncooperative and resistant and may even hide potentially serious deficiencies for fear of disclosure and possible discipline.

The timeworn work adage might be paraphrased as follows: “If a security audit is worth doing, it’s worth doing well.” Given the consequences of poorly conducted audits, security audits should be conducted *only* if they can be conducted thoroughly, carefully, thoughtfully, and instructively by experienced persons.