

Building a Forensic Capability

PRACTICE OBJECTIVE

This objective is designed for IT organizations to build a forensic capability. The objective of forensics is to enable an organization to identify the root cause of a problem. The problem can be ineffective processes, or it can be identifying individuals who circumvented IT security processes.

Many IT organizations have grown up fixing the results of a problem rather than the root cause of a problem. For example, if computer code is wrong in a program, it needs to be identified and corrected. However, correcting computer code will not remedy the cause of the problem, which most believe is a process problem. Thus, the primary use for forensics by IT quality professionals will be investigating process problems.

Forensics can also be used to identify individuals whose actions caused a loss. The actions by the individual may be intentional, which could be criminal, or unintentional on the part of the individual because that individual did not understand or follow the appropriate process.

PRACTICE TUTORIAL

Over the last decade, the number of computer process problems and crimes that involve computers has grown; this has caused an increase in the number of companies and products that aim to assist enforcement in using computer-based evidence to determine the who, what, where, when, and how problems occurred. Forensic tools and techniques are most often thought of in the context of investigations and computer security incident handling—used to respond to an event by investigating suspect systems, gathering and preserving evidence, reconstructing events, and assessing the current state of an event. However, forensic tools and techniques are also useful for many other types of tasks, such as the following:

- **Operational Troubleshooting.** Many forensic tools and techniques can be applied to troubleshooting operational issues, such as finding the virtual and physical location of a host with an incorrect network configuration, resolving a functional problem with an application, and recording and reviewing the

current OS and application of configuration settings for a host.

- **Log Monitoring.** Various tools and techniques can assist in log monitoring, such as analyzing log entries and correlating log entries across multiple systems. This can assist in incident handling, identifying policy violations, auditing, and other efforts.
- **Data Recovery.** There are dozens of tools that can recover lost data from systems, including data that has been accidentally or purposely deleted or otherwise modified. The amount of data that can be recovered varies on a case-by-case basis.
- **Data Acquisition.** Some organizations use forensics tools to acquire data from hosts that are being redeployed or retired. For example, when a user leaves an organization, the data from the user's workstation can be acquired and stored in case it is needed in the future. The workstation's media can then be sanitized to remove all of the original user's data.
- **Due Diligence/Regulatory Compliance.** Existing and emerging regulations require many organizations to protect sensitive information and maintain certain records for audit purposes. Also, when protected information is exposed to other parties, organizations may be required to notify other agencies or impacted individuals. Forensics can help organizations exercise due diligence and comply with such requirements.

Organizations should ensure that their policies contain clear statements addressing all major forensic considerations, such as contacting law enforcement, performing monitoring, and conducting regular reviews of forensic policies and procedures.

At a high level, policies should allow authorized personnel to monitor systems and networks and perform investigations for legitimate reasons under appropriate circumstances. Organizations may also have a separate forensic policy for incident handlers and others with forensic roles; this policy would provide more detailed rules concerning appropriate behavior. Forensic policy should clearly define the roles and responsibilities of all people and external organizations performing or assisting with the organization's forensic activities. The policy should clearly indicate who should contact which internal

teams and external organizations under different circumstances.

Organizations should create and maintain procedures and guidelines for performing forensic tasks, based on the organization's policies and all applicable laws and regulations.

Guidelines should focus on general methodologies for investigating incidents using forensic techniques, since it is not feasible to develop comprehensive procedures tailored to every possible situation. However, organizations should consider developing step-by-step procedures for performing routine tasks. The guidelines and procedures should facilitate consistent, effective, and accurate actions, which is particularly important for incidents that may lead to prosecution or internal disciplinary actions; handling evidence in a forensically sound manner puts decision makers in a position where they can confidently take the necessary actions. The guidelines and procedures should support the admissibility of evidence into legal proceedings, including information on gathering and handling evidence properly, preserving the integrity of tools and equipment, maintaining the chain of custody, and storing evidence appropriately. Because electronic logs and other records can be altered or otherwise manipulated, organizations should be prepared, through their policies, guidelines, and procedures, to demonstrate the integrity of such records. The guidelines and procedures should be reviewed periodically, as well as when significant changes are made to the organization's policies and procedures.

Organizations should ensure that their policies and procedures support the reasonable and appropriate use of forensic tools.

Organizations' policies and procedures should clearly explain what forensic actions should and should not be performed under various circumstances, as well as, describe the necessary safeguards for sensitive information that might be recorded by forensic tools, such as passwords, personal data (e.g., Social Security numbers), and the contents of e-mails. Legal advisors should carefully review all forensic policy and high-level procedures.

Organizations should ensure that their IT professionals are prepared to participate in forensic activities.

IT professionals throughout an organization, especially incident handlers and other first responders to incidents, should understand their roles and responsibilities for forensics, receive training and education on forensic-related policies and procedures, and be prepared to cooperate with and assist others when the technologies that they are responsible for are part of an incident or other event. IT professionals should also consult closely with legal counsel both in general preparation for forensics activities, such as determining which actions IT professionals should and should not perform, and discussing specific forensics situations. In addition, management should be responsible for supporting forensic capabilities, reviewing and approving forensic policy, and approving certain forensic actions, such as taking mission-critical systems off-line.

PRACTICE WORKBENCH

A workbench for building a forensic capability in IT organizations begins when IT management recognizes the need for forensics. Forensics is the process that will enable IT professionals to identify the root cause of a problem or the individual who caused the problem. QAI believes that the IT quality assurance function should be assigned the responsibility of building and operating a forensic capability.

There are four steps to building an effective forensic capability (see Figure 1). These four steps produce the four deliverables from this work practice. The steps and deliverables are:

1. Define a forensic policy.
2. Define the roles and responsibilities in performing forensic activities.
3. Staff the function to achieve the policy and accomplish the defined roles and responsibilities.
4. Develop the appropriate procedures to perform forensics including the necessary tools.

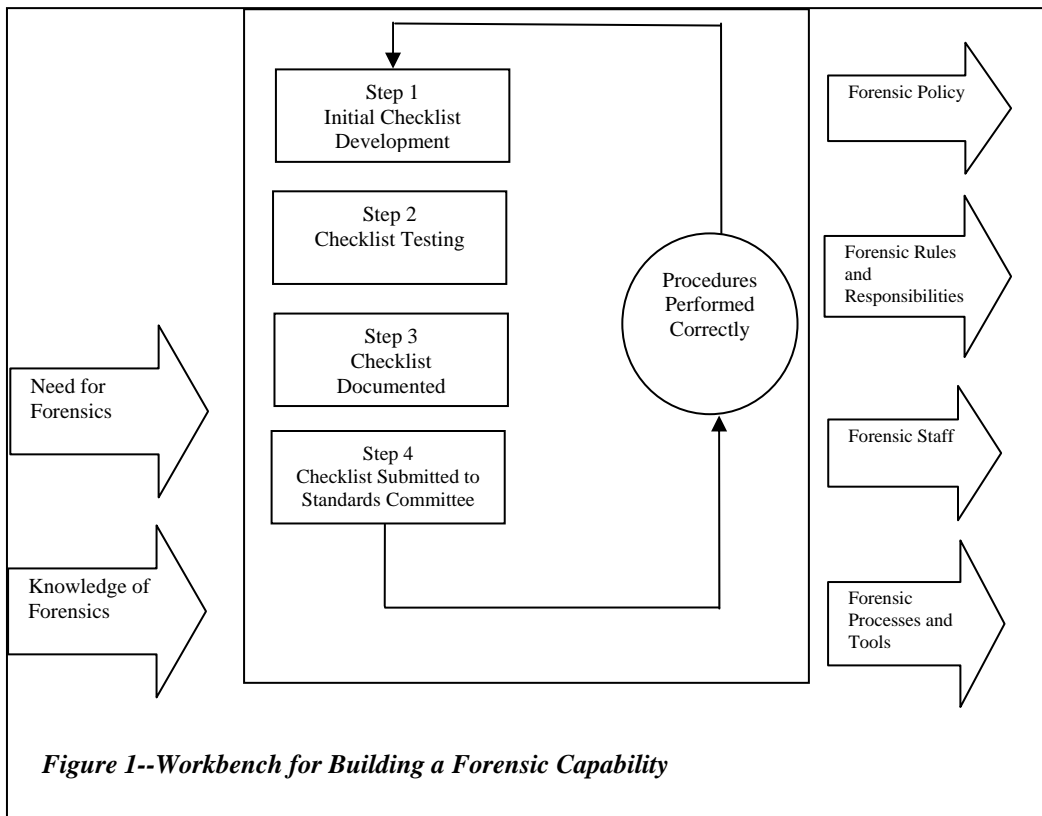


Figure 1--Workbench for Building a Forensic Capability

Step 1—Define the Forensics Policy

Organizations should ensure that their policies contain clear statements that address all major forensic considerations, such as contacting law enforcement, performing monitoring, and conducting regular reviews of forensic policies, guidelines, and procedures. At a high level, policies should allow authorized personnel to monitor systems and networks and perform investigations for legitimate reasons under appropriate circumstances. Organizations may also have a separate policy for

INPUT PRODUCTS

There are two input products to this practice. The first was described in the workbench, which is IT management’s recognition of the need for forensic capability. The second input is a knowledge of forensics. The individual assigned to build the forensic capability is the one who requires this knowledge.

There are many courses, books, and articles on computer forensics. Unfortunately, for quality assurance professionals, most of these educational materials are focused on the criminal aspect of forensics. However, for most IT organizations, the big payback from forensics will be identifying the root cause of process problems and fixing the process. Organizations specifically wanting knowledge on the use of forensics for investigating work processes, should contact QAI for an in-house course on process forensics.

IMPLEMENTATION PROCEDURES

The implementation of this practice involves the following four steps:

incident handlers and others with forensic roles; this policy would provide more detailed rules for appropriate behavior. Such personnel should be familiar with and understand the policy. Policies may need to be updated frequently, particularly for organizations that span many jurisdictions, because of changes to laws and regulations, as well as, new court rulings. In addition, the organization’s forensic policy should be consistent with the organization’s other policies, including policies related to reasonable expectations of privacy.

Step 2—Define Roles and Responsibilities

Forensic policy should clearly identify the roles and responsibilities of all people performing or assisting with the organization’s forensic activities. This should include actions performed during both incident handling and routine work activities (e.g., system administration, network troubleshooting). The policy should include all internal teams that may participate in forensic efforts and external organizations, such as law enforcement agencies, outsourcers, and incident response organizations. The policy should clearly indicate who should contact which internal teams and external organizations under different circumstances.

In most IT organizations, there are only two roles: the manager of the forensic activity and the forensic analyst. QAI recommends that the forensic manager be the quality assurance manager and the forensic analyst be the quality assurance analyst. (NOTE: In 2009, the Common Body of Knowledge for Quality Assurance will include a section on forensics.)

The emphasis in this step will be on the specific responsibilities the forensics manager and forensic analyst have. Much of those responsibilities will define with whom the forensic analyst interacts, how information will be protected, and how incidents will be handled.

Step 3—Staffing for Forensics

Practically every organization needs to have some capability to perform computer and network forensics. Without such a capability, an organization will have difficulty determining what events have occurred within its systems and networks, such as exposures of protected, sensitive data. Although the extent of this need varies, the primary users of forensic tools and techniques within an organization usually can be divided into the following three groups:

1. **Forensic analysts**—This group includes the investigators within an organization responsible for investigating allegations of misconduct and/or process problems.
2. **IT Professionals**—This group includes technical support staff and system, network, and security administrators. They use a small number of forensic techniques and tools specific to their area of expertise during their routine work (e.g., monitoring, troubleshooting, data recovery).
3. **Incident Handlers**—This group responds to a variety of computer security incidents, such as unauthorized data access, inappropriate system usage, malicious code infections, and denial of service attacks. Incident handlers typically use a wide variety of forensic techniques and tools during their investigations.

Many organizations rely on a combination of their own staff and external parties to perform forensic tasks. For example, some organizations perform standard tasks themselves and use outside parties only when specialized assistance is needed. Even

organizations that want to perform all forensic tasks themselves usually outsource the most demanding ones, such as sending physically damaged media to a data recovery firm for reconstructions or having specially trained law enforcement personnel or consultants collect data from an unusual source (e.g., cell phones). Such tasks typically require the use of specialized software, equipment, facilities, and technical expertise that most organizations cannot justify the high expense of acquiring and maintaining. Organizations should determine in advance which actions should be performed by law enforcement officials. Also, when expert testimony is needed for legal proceedings, organizations might seek external assistance.

When deciding which internal or external parties should handle each aspect of forensics, organizations should keep the following factors in mind:

- **Cost**—There are many potential costs. Software, hardware, and other equipment used to collect and examine data may carry significant costs (e.g., purchase price, software updates and upgrades, maintenance), and may also require additional physical security measures to safeguard them from tampering. Other significant expenses involve staff training and labor costs, which are particularly significant for dedicated forensic specialists. In general, forensic actions that are rarely needed might be more cost-effectively performed by an external party, whereas actions that are needed frequently, might be more cost-effectively performed internally.
- **Response Time**—Personnel located on-site might be able to initiate computer forensic activity more quickly than could off-site personnel. For organizations with geographically dispersed physical locations, off-site outsourcers located near distant facilities might be able to respond more quickly than personnel located at the organization's headquarters.
- **Data Sensitivity**—Because of data sensitivity and privacy concerns, some organizations might be reluctant to allow external parties to image hard drives and perform other actions that provide access to data. For example, a system that contains traces of an incident might also contain health care information, financial records, or other sensitive data; an organization

might prefer to keep that system under its own control to safeguard the privacy of the data. On the other hand, if there is a privacy concern within the team, for example if an incident is suspected to involve a member of the incident handling team, use of an independent third-party to perform forensic actions would be preferable.

Incident handlers performing forensic tasks need to have a reasonably comprehensive knowledge of forensic principles, guidelines, procedures, tools, and techniques, as well as, anti-forensic tools and techniques that could conceal or destroy data. It is also beneficial for incident handlers to have expertise in information security and specific technical subjects, such as the most commonly used operating systems, file systems, applications, and network protocols within the organization. Having this type of knowledge facilitates faster and more effective responses to incidents. Incident handlers also need a general, broad understanding of systems and networks so that they can determine quickly which teams and individuals are well-suited to providing technical expertise for particular forensic efforts, such as examining and analyzing data for an uncommon application.

Individuals performing forensics might need to perform other types of tasks as well. For example, if the results of an investigation are used in a court of law, incident handlers may be called upon to provide testimony and corroborate their findings. Incident handlers might provide training courses in forensics to technical support staff, system and network administrators, and other IT professionals. Possible training topics include an overview of forensics tools and techniques, advice on using a particular tool, and the signs of a new type of attack. Incident handlers might also want to have interactive sessions with groups of IT professionals to hear their thoughts on forensics tools and identify potential shortcomings in existing forensics capabilities.

On an incident handling team, more than one team member should be able to perform each typical forensic activity so that the absence of any single team member will not severely impact the team's abilities. Incident handlers can train each other in the use of forensic tools and other technical and procedural topics. Hands-on exercises and external IT and forensic training courses can also be helpful in

building and maintaining skills. In addition, it might be beneficial to have team members see demonstrations of new tools and technologies or try out forensic and anti-forensic tools in a lab. This can be particularly useful in familiarizing incident handlers with the collection, examination, and analysis of data from devices such as cell phones and PDAs. Incident handlers need to stay current with new forensic technologies, techniques, and procedures.

Interactions with Other Teams

It is not feasible for any one person to be well-versed in every technology (including all software) used within an organization; therefore, individuals performing forensic actions should be able to reach out to other teams and individuals within their organization as needed for additional assistance. For example, an incident involving a particular database server might be handled more efficiently if the database administrator were available to provide background information, answer technical questions, and provide database documentation and other reference material. Organizations should ensure that IT professionals throughout the organization, especially incident handlers and other first responders to incidents, understand their roles and responsibilities for forensics, receive ongoing training and education on forensic-related policies, guidelines, and procedures, and are prepared to cooperate with and assist others when the technologies that they are responsible for are part of an incident or other event.

In addition to IT professionals and incident handlers, others within an organization may also need to participate in forensic activities in a less technical capacity. Examples include: management, legal advisors, human resources personnel, auditors, and physical security staff. Management is responsible for supporting forensic capabilities, reviewing and approving forensic policy, and approving certain forensic actions (e.g., taking a mission-critical system off-line for 6 hours to collect data from its hard drives). Legal advisors should carefully review all forensic policy and high-level guidelines and procedures, and they can provide additional guidance when needed to ensure that forensic actions are performed lawfully. The human resources department can provide assistance in dealing with employee relations and handling internal incidents. Auditors can help determine the economic impact of an incident,

including the cost of forensic activity. Physical security staff can assist in gaining access to and physically securing evidence. Although these teams often do not play a prominent role in the forensic process, the services that these teams provide can be beneficial.

To facilitate inter-team communications, each team should designate one or more points-of-contact. These individuals are responsible for knowing the expertise of each team member and directing inquiries for assistance to the appropriate person. Organizations should maintain a list of contacts that the appropriate teams can reference as needed. The list should include both standard (e.g., office phone) and emergency (e.g., cell phone) contact methods.

Step 4—Develop Forensic Processes

All the forensic processes are comprised of the following basic phases:

- **Collection**—The first phase of the process is to identify, label, record, and acquire data from the possible sources of relevant data, while following guidelines and procedures that preserve the integrity of the data. Collection is typically performed in a timely manner because of the likelihood of losing dynamic data such as current network connections, as well as losing data from battery-powered devices (e.g., cell phones, PDAs).
- **Examination**—The second phase of the process involves forensically processing large amounts of collected data using a combination of automated and manual methods to assess and extract data of particular interest, while preserving the integrity of the data.
- **Analysis**—The next phase of the process is to analyze the results of the examination, using legally justifiable methods and techniques, to derive useful information that addresses the questions that were the reason for performing the collection and examination.
- **Reporting**—The final phase of the process is reporting the results of the analysis, which may include describing the actions used, explaining how tools and procedures were selected, determining what other actions need to be performed (e.g., forensic examination of

additional data sources, securing identified vulnerabilities, improving existing security controls), and providing recommendations for improvement to policies, guidelines, procedures, tools, and other aspects of the forensic process. The formality of the reporting step varies greatly depending on the situation and who will receive the report.

There are many models for the forensic process. Although the exact phases of the models vary somewhat, the models reflect the same basic principles and the same overall methodology. Models differ primarily in how granular each phase of the process is and in the terms used for specific phases. The model presented in this practice offers a simple way of looking at the phases. Organizations should choose the specific forensic model that is most appropriate for their needs.

Providing Guidance for Forensic Tool Use

Incident handlers are IT professionals, such as system and network administrators and others within an organization who use forensic tools and techniques for a variety of reasons. Although the technologies have many benefits, they can also be misused accidentally or intentionally to provide unauthorized access to information or to alter or destroy information, including evidence of an incident. In addition, the use of certain forensic tools may not be warranted in some situations (for example, a minor incident probably does not merit hundreds of hours of data collection and examination efforts).

To ensure that tools are used reasonably and appropriately, the organization's policies, guidelines, and procedures should clearly explain what forensic actions should and should not be performed under various circumstances. For example, a network administrator should be able to monitor network communications on a regular basis to solve operational problems but should not read users' e-mail unless specifically authorized to do so. A help desk agent might be permitted to monitor network communications for a particular user's workstation to troubleshoot an application problem but not be permitted to perform any other network monitoring. Individual users might be forbidden from performing any network monitoring under any circumstances. Policies, guidelines, and procedures should clearly

define the specific actions that are permitted and forbidden for each applicable role under normal circumstances (e.g., typical duties) and special circumstances (e.g., incident handling).

Policies, guidelines, and procedures should also address the use of anti-forensic tools and techniques. Anti-forensic software is designed to conceal or destroy data so that others cannot access it. There are many positive uses for anti-forensic software, such as removing data from computers that are to be donated to charity and removing data cached by Web browsers to preserve a user's privacy. However, like forensic tools, anti-forensic tools can also be used for malicious reasons. Therefore, organizations should specify who is permitted to use such tools and under what circumstances.

Because forensic tools may record sensitive information, policies, guidelines, and procedures should also describe the necessary safeguards for the information. There should also be requirements for handling inadvertent exposures of sensitive information, such as an incident handler seeing passwords or patient medical information.

Supporting Forensics in the Information System Life Cycle

Many incidents can be handled more efficiently and effectively if forensic considerations have been incorporated into the information system life cycle. Examples of such considerations are as follows:

- Performing regular backups of systems and maintaining previous backups for a specific period of time
- Enabling auditing on workstations, servers, and network devices
- Forwarding audit records to secure centralized log servers
- Configuring mission-critical applications to perform auditing, including recording all authentication attempts
- Maintaining a database of file batches for the files of common OS and application deployments, and using file integrity checking software on particularly important assets
- Maintaining records (e.g., baselines) of network and systems configurations

- Establishing data retention policies that support performing historical reviews of system and network activity, complying with requests or requirements to preserve data relating to ongoing litigation and investigations, and destroying data that is no longer needed

Most of these considerations are extensions of existing provisions in the organization's policies and procedures, so they are typically specified within the relevant individual documents instead of a centralized forensics policy.

Guidelines and Procedures

An organization should create and maintain guidelines and procedures for performing forensic tasks, based on the organization's policies, incident response staffing models, and other teams identified as participants in forensic activities. Even if the activities are performed by external parties, the organization's internal staff will still interact with them and participate to some extent in the activities, such as notifying the external party of a need for assistance, granting physical or logical access to systems, and securing an incident scene until an investigator arrives. The internal staff should work closely with the external parties to ensure that the organization's policies, guidelines, and procedures are understood and followed.

An organization's forensic guidelines should include general methodologies for investigating an incident using forensic techniques, since it is not feasible to develop comprehensive procedures tailored to every possible situation. However, organizations also should consider developing step-by-step procedures for performing routine tasks, such as imaging a hard disk, capturing and recording volatile information from systems, or securing physical evidence (e.g., removable media). The goal for the guidelines and procedures is to facilitate consistent, effective, and accurate forensic actions, which is particularly important for incidents that may lead to prosecution or internal disciplinary actions. Because electronic logs and other records can be altered or otherwise manipulated, organizations should be prepared, through their policies, guidelines, and procedures, to demonstrate the integrity of such records.

Information is rapidly migrating to a form in which all the information assets exist in electronic form. In both

the public and private sectors, it is increasingly important to demonstrate conclusively the authenticity, credibility, and reliability of electronic records, such as the performance of a specific action or decision or the existence of a certain item of information. Business records have normally been treated as equivalent to originals. Increasingly, some in the legal and forensic communities are concerned with the ease at which electronic records can be created, altered, or otherwise manipulated. In addition, various compliance initiatives in the public and private sectors are making it increasingly important to demonstrate the integrity of electronic records. With the explicit caveat that such issues are matters for discussion with legal counsel and senior IT officials and well beyond the scope of this publication, the use of sound, documented, and reasonably explicable forensic techniques coupled with other methods, such as log retention and analysis, is an important resource for decision makers as well as for incident handlers.

Forensic guidelines and procedures should be consistent with the organization's policies and all applicable laws. Organizations should include technical experts and legal advisors in the development of guidelines and procedures as a quality assurance measure. Management should also be involved in guideline and procedure development, particularly in ensuring that all major decision-making points are documented that the proper course of action is defined so that decisions are made consistently.

The guidelines and procedures should support the admissibility of evidence into legal proceedings, including information on gathering and handling evidence properly, preserving the integrity of tools and equipment, maintaining the chain of custody, and storing evidence securely. Although it may not be feasible to record every event or action taken in response to an incident, having a record of the major events and actions taken helps ensure that nothing has been overlooked and helps explain to others how the incident was handled. This documentation can be useful for case management, report writing, and testifying. Keeping a record of the dates and times that people worked on an incident, including the time needed to recover systems, can also help calculate the costs of damages. Also, handling evidence in a forensically sound manner puts decision makers in a position where they can confidently take the necessary actions.

It is also important to maintain the guidelines and procedures once they are created so that they remain accurate. Management should determine how frequently the guidelines and procedures should be reviewed (generally, at least annually). Reviews should also be conducted whenever the team's policies, guidelines, and procedures undergo significant changes. When a guideline or procedure is updated, the previous version should be archived for possible future use in legal proceedings. Guideline and procedure reviews should include the same teams that participate in their creation. In addition to performing reviews, organizations might choose to conduct exercises that help to validate the accuracy of certain guidelines and procedures.

CHECK PROCEDURES

Individuals new to forensics may implement a step based more on the wording in the procedure as opposed to the intent of the procedure. The objective of quality control in building a forensic capability is to provide the individual responsible for building that capability insight into the intent of the procedures for building a forensic capability.

The quality control questions are included on Workpaper #1. These are used to determine that the process for building a forensic capability was performed reasonably. A yes response indicates that the procedure was performed correctly, and a no response indicates that additional action may be warranted. Each no response should be investigated and resolved before preparing the deliverables.

DELIVERABLES

There are a minimum of four deliverables from this work practice, which are:

1. A policy on forensics and supporting policies, as needed, for example for incident handlers
2. The roles and responsibilities for individuals who will be involved in forensic investigation
3. The method in which the forensics team will be staffed, including other people within the organization and external to the organization
4. Forensics work processes and supporting forensic tools

USAGE TIPS

Six guidelines on establishing and organizing a forensic capability are as follows:

1. **Organizations should have a capability to perform computer and network forensics.** Forensics is needed for various tasks within an organization, including investigating crimes and inappropriate behavior, reconstructing computer security incidents, troubleshooting operational problems, supporting due diligence for audit record maintenance, and recovering from accidental system damage. Without such a capability, an organization will have difficulty determining what events have occurred within its systems and networks, such as exposures of protected, sensitive data. Also, handling evidence in a forensically sound manner puts decision makers in a position where they can confidently take the necessary actions.
2. **Organizations should determine which parties should handle each aspect of forensics.** Most organizations rely on a combination of their own staff and external parties to perform forensic tasks. Organizations should decide which parties should take care of which tasks based on skills and abilities, cost, response time, and data sensitivity.
3. **Incident handling teams should have robust forensic capabilities.** More than one team member should be able to perform each typical forensic activity. Hands-on exercises and IT and forensic training courses can be helpful in building and maintaining skills, as can demonstrations of new tools and technologies.
4. **Many teams within an organization should participate in forensics.** Individuals performing forensic actions should be able to reach out to other teams and individuals within an organization, as needed, for additional assistance. Examples of teams that may provide assistance in these efforts include IT professionals, management, legal advisors, human resources personnel, auditors, and physical security staff. Members of these teams should understand their roles and responsibilities in forensics, receive training and education on forensic-related policies, guidelines, and procedures, and be prepared to cooperate with and assist others on forensic actions.
5. **Forensic considerations should be clearly addressed in policies.** At a high level, policies should allow authorized personnel to monitor systems and networks and perform investigations for legitimate reasons under appropriate circumstances. Organizations may also have a separate forensic policy for incident handlers and others with forensic roles that provides more detailed rules for appropriate behavior. Everyone who may be called upon to assist with any forensic efforts should be familiar with and understand the forensic policy. Additional policy considerations are as follows:
 - a. Forensic policy should clearly define the roles and responsibilities of all people performing or assisting with the organization's forensic activities. The policy should include all internal and external parties that may be involved and should clearly indicate who should contact which parties under different circumstances.
 - b. The organization's policies, guidelines, and procedures should clearly explain what forensic actions should and should not be performed under normal and special circumstances and should address the use of anti-forensic tools and techniques. Policies, guidelines, and procedures should also address the handling of inadvertent exposures of sensitive information.
 - c. Incorporating forensic considerations into the information system life cycle can lead to more efficient and effective handling of many incidents. Examples include performing auditing on shots and establishing data retention policies that support performing historical reviews of system and network activity.
6. **Organizations should create and maintain guidelines and procedures for performing forensic tasks.** The guidelines should include general methodologies for investigating an incident using forensic techniques, and step-by-step procedures should explain how to perform routine tasks. The guidelines and procedures should support the admissibility of evidence into legal proceedings. Because electronic logs and other records can be altered or otherwise manipulated, organizations should be prepared, through their policies, guidelines, and procedures, to demonstrate the reliability and

integrity of such records. The guidelines and procedures should also be reviewed regularly and maintained so that they are accurate.

Workpaper #1—Quality Control Checklist for Building a Forensic Capability

	ITEM	RESPONSE (Circle One)		COMMENTS
		Yes	No	
1.	Does the forensic policy address both process problems and criminal activities?	Yes	No	
2.	Does the policy clearly define forensics and all of the major forensic considerations?	Yes	No	
3.	Does the forensic policy, or a separate policy, address incident handlers and others with forensic roles?	Yes	No	
4.	Does the forensic policy address how criminal investigations will be performed?	Yes	No	
5.	Are the roles and responsibilities for individuals involved in forensics clearly defined?	Yes	No	
6.	Do the responsibilities of those involved in forensics indicate the responsibilities with external organizations?	Yes	No	
7.	Does the staffing for forensics include both the forensics manager and analyst within the organization as well as other IT professionals and incident handlers?	Yes	No	
8.	Have the skills been defined for forensic analysts?	Yes	No	
9.	Does the IT organization have access to the knowledge needed to effectively build a forensic capability?	Yes	No	
10.	Do the type of forensic activities that will be performed by others in the organization and external to the organization include the factors of cost, response time, and data sensitivity?	Yes	No	
11.	Has the interaction with the forensic analysts and other teams been defined?	Yes	No	
12.	Has a forensic process been defined for conducting forensic investigations?	Yes	No	
13.	If so, does it include the phases of collection, examination, analysis, and reporting?	Yes	No	
14.	Have forensic tools been identified?	Yes	No	
15.	Have necessary forensic tools been acquired?	Yes	No	
16.	Has it been determined how forensic analysts will be trained in the use of those tools?	Yes	No	
17.	Will forensics be supported in the information system life cycle?	Yes	No	