Title: ENHANCED SYSTEM, METHOD AND MEDIUM FOR CERTIFYING AND ACCREDITING REQUIREMENTS COMPLIANCE UTILIZING THREAT VULNERABILITY FEED

Abstract: A computer-assisted system, medium and method of providing a risk assessment of a target system. The method includes receiving at the computer at least one of a newly encountered hardware, software and/or operating system threat, updating a requirements repository to account for the threat, updating one or more target system test procedures to account for the threat, and conducting a risk assessment of the target system.
For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.
ENHANCED SYSTEM, METHOD AND MEDIUM FOR CERTIFYING AND ACCREDITING REQUIREMENTS COMPLIANCE UTILIZING THREAT VULNERABILITY FEED

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention relates generally to the field of certification and accreditation (C&A) and, more particularly, to a computer-implemented system method and medium for C&A that enables users to tailor a sequence of requirements and/or activities that can be used to assess the risk of and/or determine the suitability of a target system to comply with at least one predefined standard, regulation and/or requirement.

Background Description

The general purpose of C&A is to certify that automated information systems, for example, adequately protect information in accordance with data sensitivity and/or classification levels. In accordance with Department of Defense (DoD) Instruction 5200.40, dated December 30, 1997, entitled DoD Information Technology Security Certification and Accreditation Process (DITSCAP), which is incorporated herein by reference in its entirety, certification can, for example, be defined as the comprehensive evaluation of the technical and non-technical features of an information technology (IT) system and other safeguards, made in support of the accreditation process, to establish the extent that a particular design and implementation meets a set of specified security requirements. Similarly, as used herein, accreditation can be defined as a formal declaration by a designated approving authority that an IT system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. In general, DITSCAP is utilized by the DoD for identifying and documenting threats and vulnerabilities that pose risk to critical information systems. DITSCAP compliance generally means that security risk posture is considered acceptable and that potential liability for system "owners" is mitigated. As used herein, a threat can be considered any circumstance or event with the potential to cause harm to an information technology system in the form of, for example, destruction, disclosure, adverse modification of data, and/or denial of service. As used herein, a vulnerability can be considered a weakness in, for example, an information system, or cryptographic
system, or components (e.g., system security procedures, hardware design, internal controls) thereof that could be exploited.

The C&A process typically involves a number of policies, regulations, guidelines, best practices, etc. that serve as C&A criteria. Conventionally, the C&A process is typically a labor intensive exercise that can require multiple skill sets over a period of time typically spanning 6-12 months. There can be, for example, several organizations and/or individuals that may be involved in the processes of selecting applicable standards, regulations and/or test procedures, and assembling test results and other information into a DITSCAP compliant package. There is therefore a need to substantially streamline and expedite the security C&A process in a manner that utilizes a robust risk assessment model, and substantially automates and enables a user to tailor a sequence of events that can be used, for example, to perform security risk assessments, certification test procedure development, system configuration guidance, and residual risk acceptance.

**SUMMARY OF THE INVENTION**

To address the deficiencies of conventional schemes as indicated above, the present invention provides a system, method and medium that substantially automates and provides users the ability to customize the security C&A process in a manner that enhances and facilitates security risk assessments, certification test procedure development, system configuration guidance, and/or residual risk acceptance.

In an exemplary embodiment, the C&A process can be automated in accordance with, for example, any of DoD’s DITSCAP requirements, National Information Assurance Certification and Accreditation Process (NIACAP) requirements, Director of Central Intelligence Directives (DCID) (e.g., DCID 6/3), and British Standard/International Standards Organization (BS/ISO) 17799. The present invention is not, however, limited to these requirements/standards, applications and/or environments, and may also be used in conjunction with other government and civilian/private sector organizations requiring risk management and/or guidance.

One or more embodiments of the present invention contemplate automating, for example, at least the DITSCAP, NIACAP, DCIS and/or BS/ISO security processes, and are directed to six primary elements: 1) gathering information, 2) analyzing requirements, 3) testing requirements, 4) managing content; 5) performing risk
assessment, and 6) generating certification documentation (based at least in part on an
assessment of the first five elements) that includes information that enables an
accreditation decision to be made.

One or more embodiments of the present invention also contemplate

substantially automating (or can be used to substantially automate) the security C&A
process for information technology based assets. A process is provided to determine
target system vulnerability to each of one or more threats, and assess network and
target system compliance with applicable regulations, standards, and/or industry best
practices.

One or more embodiments of the present invention allow one or more users to
define the network or target system configuration. This aspect of the present invention
can be automated by a network discovery and scanning utility that identifies target
system assets (e.g., workstation manufacturer and model, operating system and
version), and inventories each hardware component, its associated operating system and
software applications.

Once system configuration information has been gathered, the environment
(e.g., secret, or top secret operating environment) in which the target system operates
can be described. One or more embodiments of the present invention can automatically
engage (or select) the appropriate security requirements (with which the system must or
should comply) according to government and/or industry standards and best practices.
Appropriate test procedures can also automatically be selected by the system
corresponding to selected security requirements. The user can also manage the content
(e.g., edit) of these requirements and/or input his/her own standards/regulations and/or
additional requirements. The user can also manage the content (e.g., edit) of one or
more test procedures by, for example, adding and/or deleting test procedures to those
initially selected by the system, and/or by editing existing test procedures initially
selected by the system.

Upon completion of testing and entering test results, the present invention can
produce a risk assessment of the target system. In one or more embodiments
contemplated by the present invention, the percentage of failed requirements within
each requirements category, among other considerations, can be utilized to evaluate the
risk level of the target system as a whole.
Then, documentation can be printed that includes information that enables an accreditation decision to be made. It should be understood that the precise sequence of the various steps mentioned above can be varied.

One or more embodiments of the present invention can also receive updates pertaining to recently discovered threats, and conduct a scan of network assets, each of which, alone or in combination, can be used to assess system risk posture and/or target system compliance with, for example, one or more requirements.

One or more embodiments of the present invention also provide predefined steps for executing a C&A. This aspect of the present invention provides users the ability to customize one or more of the aforementioned six elements by, for example, selecting a portion of the predefined steps associated with each of one or more of the six elements.

Additional features of one or more embodiments pertain to automatically sending e-mail alerts upon, for example, the occurrence of certain C&A-related events, and a program management feature where one or more steps or events can be designated as being prerequisite to commencement of one or more other steps or events.

Before explaining at least one embodiment of the invention in detail, it is to be understood that the invention is not limited in its application to the details of construction and to the arrangements of the components set forth in the following description or illustrated in the drawings. The invention is capable of other embodiments and of being practiced and carried out in various ways.

**BRIEF DESCRIPTION OF THE DRAWINGS**

The Detailed Description will be best understood when read in reference to the accompanying figures wherein:

FIG. 1 is an exemplary high level flowchart of a method contemplated by at least some embodiments of the present invention;

FIG. 2 is an exemplary architecture of a system contemplated by at least some embodiments of the present invention;

FIG. 3 is an exemplary architecture contemplated by at least some embodiments of the present invention that can be used to provide vulnerability updates;

FIG. 4 is an exemplary architecture contemplated by at least some embodiments
of the present invention that can be used to scan a target system;

FIG. 5 is an exemplary screen display corresponding an exemplary embodiment of the present invention as shown in FIG. 1;

FIG. 6 shows an exemplary screen display that enables a user to add a new project;

FIG. 7 is an exemplary screen display that enables a user to specify settings to detect network hosts by, for example, using an enterprise management system;

FIG. 8 is an exemplary project definition screen display showing a constraint setting that can be used or specified in an automated assessment of a target system configuration;

FIG. 9 is an exemplary project definition screen display showing settings that can be used in an automated assessment of a target system configuration;

FIG. 10 is an exemplary project definition screen display showing user selection of vulnerability feed settings;

FIG. 11 is an exemplary flow chart of the requirements analysis process as contemplated by at least some embodiments of the present invention;

FIG. 12 is an exemplary screen display used to generate a security requirements traceability matrix (SRTM);

FIG. 13 is an exemplary screen display that can be used to collect system requirements and/or operating environment;

FIG. 14 is an exemplary screen display showing how a test procedure can be edited;

FIG. 15 is an exemplary screen display illustrating how a user can associate a test procedure(s) with one or more requirements;

FIG. 16 is an exemplary screen display showing how a user can add a test procedure;

FIG. 17 is an exemplary screen display showing how a user can edit a regulation;

FIG. 18 is an exemplary screen display showing how a user can edit threats;

FIG. 19 is an exemplary display that can be used to edit hardware, software and/or operating system lookups;

FIG. 20 is an exemplary screen display that enables a user to add and/or edit
definitions used for a C&A project.

FIG. 21 is an exemplary high level flow diagram of a risk assessment method according to at least some embodiments contemplated by the present invention;

FIG. 22 is an exemplary flow diagram of a risk assessment method contemplated by at least some embodiments of the present invention;

FIG. 23 is an exemplary screen display showing illustrative threat categories;

FIG. 24 is an exemplary screen display that enables a user to view the setting for a requirements category element, along with a default level of risk for each threat element; FIGs. 25a, 25b and 25c show exemplary risk tables that can be used to calculate target system risk;

FIG. 26 is an exemplary flow diagram of a method of assessing overall system risk in accordance with at least some embodiments contemplated by the present invention;

FIG. 27 shows an exemplary screen display that enables a user to print a complete project report or components thereof;

FIG. 28 is an exemplary screen display that enables the React component of the present invention to be utilized in the C&A for a project;

FIG. 29 is an exemplary screen display that can be used to view project names and related information;

FIG. 30 is an exemplary screen display that enables a user to edit project information;

FIG. 31 is an exemplary screen display that can be used to assign a role to a user;

FIG. 32 is an exemplary screen display that can be used to assign or add various roles to a project;

FIG. 33 is an exemplary screen display that can be used to specify access rights and notification for various tasks;

FIG. 34 is an exemplary screen display that can be used to associate one or more Process Steps (PSs) with a task;

FIG. 35 is an exemplary screen display that shows project personnel and related information;

FIG. 36 is an exemplary flow diagram of the task manager process;
FIG. 37 illustrates one example of a central processing unit for implementing a computer process in accordance with a computer implemented embodiment of the present invention;

FIG. 38 illustrates one example of a block diagram of internal hardware of the central processing unit of FIG. 37;

FIG. 39 is an illustrative computer-readable medium upon which computer instructions can be embodied;

FIG. 40 is an exemplary network implementation of the present invention; and

FIG. 41 is an exemplary entity relationship diagram that describes the attributes of entities and the relationship among them.

DETAILED DESCRIPTION

Referring now to the drawings, and more particularly to FIG. 1, a high level flow diagram is shown that provides an overview of a method according to one or more embodiments of the present invention. In the first step, information is gathered pertaining to the system or network undergoing C&A, as indicated by step 100. The information gathered typically relates to a description of the system to be certified, and its respective components and operating environment (e.g., workstation manufacturer and model, operating system and version, secret, or top secret operating environment, etc.). One or more embodiments of the present invention also contemplate receiving updates pertaining to recently discovered threats, and can conduct a scan of network assets, each of which, alone or in combination, can be used to assess system risk posture and/or target system compliance with, for example, one or more requirements.

As indicated above, aspects of at least some embodiments of the present invention are described in accordance with DoD's DITSCAP requirements. In accordance with DITSCAP, and as used herein, risk can be defined as a combination of the likelihood that a threat will occur, the likelihood that a threat occurrence will result in an adverse impact, and the severity of the resulting impact. Also in accordance with DITSCAP, vulnerability can be defined as a weakness in, for example, an information system, a cryptographic system, and/or components thereof (e.g., system security procedures, hardware design, internal controls) that could be exploited. As used herein, susceptibility can be defined, for example, as the potential (e.g., zero or some finite possibility) that a vulnerability exists on the system.
However, it should be understood that such description is only by way of example, and that the present invention contemplates use with regard to any number of types of requirements or environments (e.g., NIACAP, DCID and/or BS/ISO requirements or processes). In addition, within its use with regard to DITSCAP requirements, it should be understood that many of the various aspects and selection options are also exemplary, as is the fact that information is shown as being entered via a screen display. Further information pertaining to the system and method according to the present invention can be found in the following document: Xacta WEB C&A™ User’s Guide, Version 3.3, Copyright 2002, available from Xacta Corporation, Ashburn, VA. A copy of this document is incorporated herein by reference in its entirety.

The requirements analysis generally involves selecting (by a human and/or some automated procedure) a list of standards and/or regulations (or portions thereof) that the system must, or should, comply with, as indicated by step 102. Selection of additional standards/regulations and/or requirements by a user is also contemplated. At least some embodiments of the present invention also contemplate automatically displaying/listing each requirement. The requirement(s) can be displayed, for example, in the form of a security requirements traceability matrix (SRTM) (as shown, for example, in FIG. 12). As known to those skilled in the art, a SRTM can be used to trace project lifecycle (e.g., from identification through implementation) activities (e.g., testing requirements) and/or tasks to the project requirements, and can generally be derived from the selected set of standards and/or regulations with which the system must comply. A SRTM can thus be used to ensure that project objectives and/or requirements are satisfied and/or completed.

Once information is gathered 100 and the requirements to be complied with (as identified, for example, in requirements analysis 102) are provided, the system can intelligently select a set of test procedures (against which the system can be tested), as is indicated by step 104. The test procedures are selected in a manner so that successful completion of the test procedures can render the system undergoing C&A to satisfy the SRTM requirements. Additionally, the user can customize one or more test procedures by, for example, adding, editing and/or deleting test requirements.

At step 106, the user can (continue to) add, delete and/or edit requirements.
selected at step 102 and/or test procedures selected at step 104. That is, the user can add, delete and/or edit requirements selected at step 102 and/or test procedures selected at step 104 during performance of these steps, as well as subsequent to these steps upon, for example, receiving a new or updated test procedure and/or a new or updated requirement. The user can edit selected requirements and/or test procedures by using, for example, a conventional display monitor.

Upon completion of testing, the risk assessment step, as indicated by step 108, involves assessing for each requirement failure (should any exist) the vulnerability of the system, as well as the level of the threat as determined by the information gathered. The present invention provides a scheme whereby system vulnerabilities can be continuously assessed by considering newly discovered threats, and updating test requirements and procedures to account for such threats. One or more target systems can then be tested against the threats in accordance with updated test procedures that account for such threats.

The risk assessment 108 provides as output an estimate of the risk level for each requirement category. Each failed requirement within a requirement category is collectively considered and used to evaluate the risk level of the system as a whole. Then, documentation can be printed 110 that includes information pertaining to the first five elements that would enable an accreditation decision (manual or automated) to be made based on the inputs and outputs respectively provided and generated in steps 100, 102, 104, 106, and/or 108. Each step shown in FIG. 1 (i.e., 100, 102, 104, 106, 108 and 110) will be discussed in further detail herein.

FIG. 2 is an exemplary architecture of a system 200 in accordance with at least some embodiments of the present invention. Additional features pertaining to FIG. 2 will be discussed in connection with subsequent figures. System 200 comprises assessment module 201, detect module 222, knowledge base 228, publisher 230, and hosts 224. Hosts 224 represent any of one or more hosts (e.g., computers, monitors, routers, printers, and the like, within network 236). A host generally should (or is required to) comply with one or more selected security requirements, and be tested to determine compliance with such requirement(s). That is, hosts 224 can be (or can be part of) the target system being tested (for, e.g., subsequent accreditation).

One or more screen displays (not shown) can be provided that enable a user to
describe and store the identification of hosts 224 that may be associated with, for example, network 236. In addition, a user can also specify hosts 224 that are within the network, but are outside of the accreditation boundary (i.e., not included in the accreditation). This category might include such equipment/services as, for example, a domain naming service (DNS) used to translate the host names to IP addresses. The DNS might not be part of the atomic system being accredited, but is required for most communication activities. The following exemplary fields can be provided in an exemplary screen display: Accreditation Boundary Name (a name associated with the external system component), and Accreditation Boundary Description (a detailed description of the external system component, which can include the function that this component/service provides the system being accredited and its relationship to the system).

Within assessment module 201, event module 214 communicates with react module 204, risk module 234, delta check module 208, update scheduler 212, publisher 216, persistence layer 218, and administration module 230 to accept, monitor and/or coordinate events between the various modules. Event module 214 can be implemented, for example, as a conventional queue to process the various inputs and outputs shown.

One or more computing devices 220 (e.g., a conventional personal computer) can be provided that interface with assessment module 201 by way of a conventional HyperText Transport Protocol (HTTP) listener 202 which, in turn, can communicate with presentation manager 206. Presentation manager 206 coordinates and manages presentation of the various screen displays provided by, for example, react module 204 and/or risk module 234 that can be displayed on a conventional display monitor 221 associated with computing device 220.

Presentation manager 206 can communicate with, for example, update scheduler 212, which allows users (using, for example, computing device 220) to make appropriate settings that enable update scheduler 212 to receive new threats and/or test package updates that can be stored, for example, in knowledge base 228. Test package updates can be utilized to determine the degree of compliance with (or how susceptible hosts 224 are) to any newly detected threats. Knowledge base 228 will also receive updated regulations and requirements. These documentation changes, in conjunction
with recently discovered changes to the equipment inventory/configuration of hosts 224, can be used to update a project test matrix (e.g., a list of test procedures that can be used to assess compliance of hosts 224 with one or more requirements and/or regulations). Changes to the project test matrix can be used to update the level of risk associated with individual risk elements, and the overall risk profile of the project.

Presentation manager 206 can also communicate with administration module 230 to, for example, update test procedures in knowledge base 228. Administrative module 230 facilitates communication between presentation manager 206 and persistence layer 218. Persistence layer 218 can be used, for example, to facilitate adding new requirements, editing existing requirements, adding a new test procedure and/or editing an existing test procedure to (or within) knowledge base 228. Persistence layer 218 can communicate with event module 214 which, in turn can, for example, notify react module 204 to alert an analyst that a new test is to be conducted.

Similarly, administration module 230 can communicate with event module 214 when, for example, a user changes times for the automated reexamination of the hardware and/or software configuration of host 224. In this case, event module 214 can notify delta check module 208 to activate detect module 222 by using communications module 210. Delta check module 208 can communicate with detect module 222 at specified (e.g., predetermined) intervals. Detect module 222 can search for new equipment (not shown) within network 236. When a run of Detect module 222 is complete, test procedures, test results, risk elements, and risk levels, are updated in knowledge base 228, as appropriate. For example, target system risk can be appropriately updated to indicate that the target system has not been tested for compliance with a newly discovered threat (having or exposing a corresponding target system vulnerability). Similarly, system risk can be appropriately updated to indicate that the system has been tested for compliance with a newly detected threat.

Update scheduler 212 can also generate events related to user notifications. As will be discussed herein, react module 204 can send, for example, an e-mail to one or more project personnel notifying them that, for example, a new test must (or should) be completed to ensure that (a newly detected) system configuration complies with (newly detected or updated) regulations or requirements.

In one or more embodiments of the present invention, and as will be discussed
herein in further detail, detect engine 222 utilizes (or accesses) several network
detections mechanisms or protocols to detect changes in host 224 configuration.
Computing device 220 can be used to facilitate configuration of the various operational
controls and settings of the detect module 222.

Once test results have been entered and stored in knowledge base 228, risk
module 234 can be used to conduct a risk assessment (as will be discussed herein) of
individual requirement categories, as well as of a target system as a whole (e.g., hosts
234). Upon completion of the risk assessment, publisher module 216 can use printer
230 to print (publish) at least a portion of a report indicating outcomes and/or risk
profile of the tested target system.

FIG. 3 is an exemplary architecture contemplated by at least some embodiments
of the present invention that can be used to provide vulnerability updates. As shown in
FIG. 3, update scheduler 212 can receive updates from registration server 336 and/or
from e-mail server 234. Update server 332 is a master repository that can include
known threats, including any recently discovered threats. When update server 332
receives an indication that a new threat has been discovered, content database 316 is
updated to reflect any newly discovered threats. Such threats can be entered manually
(by, e.g., computing device 360) into content database 316, or by way of a network
connection (not shown).

In one or more embodiments of the present invention, update server 332 can
notify e-mail server 234 that one or more new threats have been discovered. Any new
updates threats, regulations, and the like, can also be transmitted in the e-mail. In
addition, a user can access registration server 336 to request update packages (e.g., new
test procedures that can test for new system vulnerabilities) from update server 332.

Registration server 336 can verify user credentials, and verify, for example, that
a user has a paid and updated subscription to receive updates from content database
316. With regard to registration server 336, package upload manager 304 can receive
manual updates (e.g., by a floppy drive or CD-ROM drive) of test procedures,
regulations, and the like, stored in content database 316. Live update manager 310 can
receive updates from update server 332 by, for example, a network connection. Keys
generator 306 generates keys (e.g., passwords) for client (user) use to receive updates
from update server 332. In at least some embodiments contemplated by the present
invention, users are provided with a generated key that can be typed into a field within a display screen shown on display monitor 221 to receive updates from content database 316. Licenses manager 308 adds authorized-user data to registration database 318. Project upload manager 304, keys generator 306, licenses manager 308, and live update manager 310 provide information to registration database 318 by using database connector 312 which can provide, for example, protocol conversions and/or data normalization between the respective modules and registration database 318.

A user using a computing device 220 can access a HyperText Transport Protocol Secure (HTTPS) (or an HTTP) listener 302 to receive the latest vulnerabilities and revised test procedures and requirements from content database 316. In particular, after accessing HTTPS listener 302, licenses manager 308 will verify user privileges, and live update manager will access content management server 314 to transmit the latest vulnerabilities and revised test procedures and requirements to update scheduler 212.

Referring back to FIG. 2, update scheduler 212, using persistence layer 218, updates affected test procedures, requirements, and/or regulations in knowledge base 228, as appropriate, to reflect any new threats to which a target system (e.g., hosts 224) may be vulnerable. In addition, event module 214 can notify react module 204 of the update. In turn, react module 204 can inform, for example, affected users (e.g., analysts, administrators and/or data entry personnel) by way of administration module 230, presentation manager 206, HTTP listener 202, and browser 220. Users can then direct that another assessment of hosts 224 be performed by, for example, detect module 222. Computing device 360 can be used to, for example, manually update content database to ensure that test procedures, regulations, and the like, are updated to account for any newly discovered threats.

FIG. 4 shows aspects of detect module 222. Referring now to FIG. 4, and as contemplated by one or more embodiments of the present invention, assessment module 201 can communicate with detect module 222 by way of secure listener 404 and unsecure listener 410. When assessment module 201 indicates that a scan of a network 228 is to be performed, secure listener 404 communicates with command scheduler 406 to determine whether host(s) 224 within network 236 are to be directly scanned (by, e.g., “pinging” hosts), or whether host configuration can be obtained from
an enterprise management (EM) database containing host 228 configuration data.

If command scheduler 406 indicates that host configuration data is to be obtained from EM database 414, host 224 configuration data is transmitted from EM database 414, to EM adapter manager 412, which is configured to read the particular database configuration of EM database 414. EM adapter manager 412 transmits host 224 configuration data to secure listener 404 which, in turn, transmits that data to assessment module 201 for subsequent storage in knowledge base 228.

In scanning the network 236, plug-in manager 402, which can store known vulnerabilities, instructs scanner 312 to determine if a host 224 is susceptible to one or more vulnerabilities defined in plug-in manager 402. Vulnerabilities can be updated and/or added after they are received by update server 332.

Host manager 408 maintains a list of hosts 224 known to assessment module 201. Hosts 224 recognized by assessment module can communicate with detect module 232 by using an unsecured connection. Host(s) 224 can pulse unsecured listener 410 to indicate presence, and determine whether host(s) 224 should transmit, for example, configuration data to detect module 222. In the event that assessment module 201 determines that host(s) 224 should transmit configuration data to detect module 222, communication is established, and configuration information is transmitted, between secure listener 404 and host(s) 224.

FIG. 5 is an exemplary screen display corresponding to the steps (100, 102, 104, 106, 108, 110) provided in FIG. 1. By clicking on an icon under Open column 502, the corresponding task under the Name column 504 will be opened. Process Steps column 502 indicates the number of screen displays currently associated with a respective task. Description column 506 can be utilized to provide text describing the name of a task. State column 508 indicates whether a task is opened or closed. To change the state, a user can click on a corresponding forward arrow icon under Change State column 510. By clicking on an icon under Properties column 514, a screen display such as shown in FIG. 34, associated with a corresponding task under Name column 504, can be opened. By clicking on an icon under Copy column 516, a user can copy a task (to the same project) to, for example, edit data and/or see how new information can impact workflow (discussed with regard to FIGs. 31-36). By clicking on an icon under Delete column 518, a user can delete a task from the project. By
clicking Add icon 520, a user can add a task from another project into the existing project (shown in FIG. 5). By clicking on Copy/Replace icon 522, a user can copy a task from another project into the existing project, and replace a task of the existing project.

*Information Gathering*

FIGs. 6-10 show selected exemplary screen displays of the information gathering 100 process. Specifically, FIG. 6 shows a display that enables a user to add a new project. Fields such as Project Name* 610, Description: 620, and Subscription Key: 630 can be provided as being part of the project definition. The asterisk (*), for example, can be utilized in the various screen displays of the present invention to indicate to the user that data entry is mandatory. The Project Name* 610 field enables a user to enter a name for a project. The Description: field 620 can be used to provide a detailed description of the project (e.g., mission statement, function, features, and/or capabilities of the system being accredited). Subscription Key: 630 can be used, for example, to identify an organization and store and/or associate user access rights to a project 610.

Via the Status* selector 640, a user can designate whether the project is Active or Inactive. In accordance with at least some embodiments of the present invention, users can access at least a portion of one or more projects to which they have been granted user rights, whereas users (other than, for example, a system administrator) would not be granted access to any portion of a project having an inactive status. If a user selects the Available As Template* 650, the current project 610 can be copied and used as the baseline for another project. In such as case, the project name entered in Project Name* field 630 would, when selected by a user, appear under (or within), for example, the Tier I and/or Tier II templates 660. As used herein, a Tier I user means that the user is generally entitled to access and provide data with respect to each site of a multiple site accreditation. A Tier II user means that the user is generally entitled to access and provide data with respect to a single site of a multiple site accreditation.

FIG. 7 is an exemplary screen display enabling a user to specify settings to detect network hosts by way of an enterprise management (EM) system. As discussed with regard to FIG. 4, the present invention can utilize an EM system to detect host configurations within a network. In Engine URL* field 704, a user specifies the URL
of detect engine 222. To activate the EM option, a user can check EM Adapter: box 702, and supply appropriate information in the shown Product* 704, Version* 706, Server Address* 708, Database Name* 710, DB username* 712, and DB password* 714 fields that enable detect engine 222 to communicate with EM database 414 by way of a server (not shown) associated with EM database 414. Host Info: box 706 can be selected to enable the Host Pulse Interval: (of, for example, host 224) to be selected by using pulldown menu 716.

FIG. 8 is an exemplary project definition screen display showing how scanner constraints can be specified. In Processing Window 802, a user (e.g., a project administrator) can specify whether the scanner can operate anytime by checking the 24 hour: box 804, or during specified times, by utilizing the Start Time* 806 and End Time* 808 pulldown menus. One or more conventional techniques 814 (e.g., TCP (Transmission Control Protocol) Ping, TCP Port, UDP (User Datagram Protocol) Port, SNMP (Simple Network Management Protocol), and ICMP (Internet Control Message Protocol) Ping) can be used to permit scanning of the network 236. In addition, a user can specify which vulnerabilities can be scanned (or tested) for by checking appropriate boxes within Vulnerability Family Scan Constraints 812.

Once constraints have been specified (as discussed with regard to FIG. 8), a user can access an exemplary screen display such as shown in FIG. 9 to specify network discovery settings. As shown at Processing Window 900, Start Time: 901 and an End Time: 902 are both set to 24:00, indicating that the 24 hour box 804 has been selected. Start Time: 901 and End Time: 902 could also be determined or bounded by respective values entered at 806, 808, respectively.

A user can also specify how often a network 236 is to be scanned. For example, in Frequency* field 906, a user can specify that a network 228 is to be scanned, for example, to every n days. The Next Run Date* field 904 will indicate the next day that the network is to be scanned. Numbers other than 15 can also be utilized. A range of IP addresses to search for in EM database 414 can also be specified in IP Range* field 908.

A user can also specify that the network is to be scanned by using one or more conventional techniques 910 (e.g., TCP Ping, TCP Port, UDP Port, SNMP, and ICMP Ping), as each technique was enabled at display section 814. Host Info: box 912 can be
activated to indicate that hardware and/or software configuration information is to be obtained from hosts 226 within the range of IP addresses specified in field 808.

FIG. 10 is an exemplary project definition screen display showing user selection of vulnerability feed settings. As discussed with regard to FIG. 2, when newly discovered threats are received, they can be inserted into knowledge base 228, and compared against the current hardware and software configuration of hosts 224 within the network 236. Users can then be notified, for example, as to which hosts 224 or host components (e.g., an operating system of a particular host or hosts) may be susceptible to the new threat.

Component: pulldown menu 1002 is set to Vulnerability Feed, and Update Engine: pulldown menu 1004 (corresponding to update server 334) is set to Enabled. Host URL: 1006 corresponds to the URL of registration server 336. Update Interval: menu 1008 indicates the update frequency provided by registration server 318.

When update server 332 (corresponding to vulnerability feed engine) is enabled, vulnerabilities and newly discovered threats to which the target system (e.g., hosts) are exposed are received from update server 332. Knowledge base 228 can then be updated to reflect such newly discovered threats and attendant vulnerabilities. As will be discussed herein, react module 204 can notify a user when new vulnerabilities arrive.

In another screen display (not shown), vulnerability updates can be sent to e-mail server 334. The name of the e-mail server, type of e-mail server (e.g., Post Office Protocol (POP), Internet Message Access Protocol (IMAP)), security settings, mail checking interval, and the like can be specified in fields (not shown) similar to that shown in FIG. 10.

Requirements Analysis

The system configuration captured in step 100 of FIG. 1 is used as input for the determination of the requirements indicated by step 102. The process of editing and/or determining/selecting those requirements is shown in FIG. 11.

In an exemplary embodiment, a general purpose computer on which one or more embodiments of the present invention operates will have stored thereon or have access to a repository (e.g., knowledge base 228) of security regulations and test procedures from various government and/or civilian departments, agencies, organizations, etc. (e.g., such as those from DITSCAP). At step 1102, and based at least
in part on the information entered in step 100, pertinent regulations will be selected from this repository, upon which to build a security requirement traceability matrix (SRTM) for the C&A.

An exemplary SRTM, shown in FIG. 12, can be a mapping of one or more requirements 1206 (e.g., a paragraph 1208 within a requirement 1206) to a regulation 1210. Satisfactory completion of the respective requirements is generally considered to render the regulation satisfied. However, the user has the flexibility to view and modify 1104 the SRTM as desired to meet the specific needs of the system(s) being accredited. In one or more embodiments, when an Applicable box 1204 is checked, a user can be presented with questions (e.g., as shown in FIG. 13) which when answered, can be used to automatically generate a SRTM (as shown in FIG. 12). When a Lock box 1202 is checked, Applicability box 1204 remains checked or unchecked, as the case may be, regardless of subsequent SRTM-related questions answered (such as shown in FIG. 13).

At step 1106, and as shown in FIG. 14, a user can display and edit one or more of the test procedures associated with a SRTM requirement 1206. By using folder menu 1414, a user can associate an operating system with the test procedure. By using folder menu 1416, a user can associate installed software with the test procedure being edited. Similarly, by using folder menu 1420, a user can associate equipment with the test procedure being edited. The user can then modify and save the revised test procedure 1108 by, for example, clicking Save button 1402. The user can then either end the editing process by, for example, clicking Cancel button 1404, or continue to modify another test procedure 1110 by, for example, typing a designator for another test procedure in Name field 1406. When clicked, Reset button will reset the display to its initial (e.g., default) condition.

Still referring to FIG. 14, Scope: pulldown menu 1418 refers to the locations at which testing can occur. Using Minimum CAL Level field 1408, a user can specify a certification and accreditation level (CAL) associated with a particular process, standard or procedure (e.g., DITSCAP). Test Text field 1410 displays the text of the particular test procedure being edited. Expected Result field 1412 indicates the expected result (after testing). Finally, area 1422 indicates the method of testing (e.g., by observation, documentation and/or actual testing).
Testing

With the security requirements traceability matrix in place (a portion of which is illustratively shown in FIG. 12), the user proceeds to the testing step 104. In one or more embodiments of the present invention, user interfaces will be provided, in accordance with the steps shown in FIG. 15, for the user to: a) add and/or edit test plan information 1502, b) associate requirements to test procedures 1504, c) add and/or edit test procedures 1406, d) enter test results 1508, and/or e) publish test results 1510. Any of the above steps can be repeated as needed, as indicated in decision step 1512.

With regard to step 1508, test results can also be automatically entered into test procedures, without human input. For example, suppose a requirement exists that user passwords be at least eight characters in length. If detect module 222 scans a network 236 and determines that one or more user passwords are less than eight characters in length, detect module 222 could automatically enter (by using communications module 210, and persistence layer 218) into an applicable test procedure stored in knowledge base 228 that the test procedure (and therefore one or more associated requirements) has not been satisfied.

With regard to step 1502, a screen display (not shown) can be provided for a user to enter information such as: an expected date of a test, the planned location of the test, test resources required, test personnel required, and remarks. Step 1502 can also be performed with printing documentation at step 110.

In accordance with step 1504, a user via a screen display (not shown) can also select a test procedure to associate it with at least one requirement selected. That is, each requirement will have one or more test procedures associated with it to ensure that compliance with the requirement has been tested. A user can, for example, by using a screen display, select a source requirements document, and associate the source requirement document with one or more test procedures. Using a screen display such as shown in FIG. 16, a user can also create a new test procedure. The exemplary input fields on the screen are: Name*, 1602, Minimum C&A Level* 1604, Test Text* 1606, and Expected Result* 1608. Folder menus 1414 and 1416 can be used as discussed with regard to FIG. 14.

After the user enters the respective test procedure information into a form presented on a new menu (not shown), the user can save the procedure(s) and associate
the newly created procedure(s) with a requirement (as described above). Saving the test procedure can also be done at content management step 106.

One or more embodiments of the present invention also contemplate that tests can be edited in accordance with step 1506 by using a screen similar to that of FIG 14. The exemplary input fields on the screen are: Name*, 1406, Minimum C&A Level*, 1408, Test Text* 1410, and Expected Result* 1412.

One or more embodiments of the present invention also contemplate that test procedures can be intelligently selected by the present invention for the C&A at hand by using, for example, the system information specified in step 100 and the requirements analysis step 102. As discussed above in the context of the SRTM, one or more test procedures within the test procedure database can be mapped to, linked with, and/or otherwise associated with each of the individual requirements within each respective requirement 1206.

A user can also enter test results by using a display screen (not shown) similar to that of FIGs. 14 and 16. For example, a Results field can be provided that allows the user to enter the test result (e.g., pass or fail). A Tester field can be provided that enables the tester to provide his name, and a Date field can be provided that allows a user to enter the date(s) that the test was conducted on. Finally, a Notes field can be provided that allows a user to enter any notes or remarks pertaining to the test.

**Content Management**

As indicated at step 106, the system 200 also enables a user to manage the content of, for example, various regulations, criteria questions, acronyms, definitions, lookups, security checklists, and the like. For example, FIG. 17 is an exemplary display that enables a user to edit a regulation. The user can edit the Short Title* 1702 and Full Title* of the regulation. In addition, a user can edit or modify the Date: 1707 (e.g., publication date), Author: 1708 (or, e.g., responsible organization), Version: 1710, and URL: 1712 for the regulation (if applicable). After editing, Save button 1714 can be activated to save any changes made to any of the aforementioned fields.

FIG. 18 is an exemplary display that can be used to edit threats. For example, in Name* field 1808, an administrative user can be identified as a potential human intentional authorized threat in threat Group* field 1804. After editing, Save button 1806 can be activated to save any changes made to any of the aforementioned fields.
FIG. 19 is an exemplary display that can be used to edit lookups (e.g., known hardware, software and/or operating systems, and associated manufacturers). As shown, a user can add a new lookup by using New Lookup: field 1902. For example, a user can specify a new WinNT version in field 1902. After activating Save button 1906, the new WinNT versions could appear, for example, in WinNT folder 1904.

As shown in FIG. 20, a user can also add and/or edit definitions used for a C&A project. For example, a user can type in the term “Accreditation” in Term* field 2002. The definition will appear in Definition* field 2004, which the user can then edit and save. Any edits can be saved by activating Save button 2006.

Similar displays can be provided with regard to, for example, managing criteria questions, and project acronyms. For example, with regard to managing criteria questions, one or more screen displays can be provided that enable a user to indicate whether the system to be tested, for example, has a compartmentalized special access classification, whether employee owned computers access the network, and/or whether remote terminals access the network 224. Other screen displays can similarly be utilized to enable users to access, edit, create and/or save material pertinent to the project C&A.

Risk Assessment

Once the testing step 104 has been completed and results have been recorded, the risk assessment step 108 commences, as indicated by sub-headings a-d below.

FIG. 21 provides an overview of the risk assessment process. At step 2102, requirements are selected, as has been discussed, for example, with regard to step 102 and FIGs. 11-15. At step 2104, test procedures are generated and/or selected. For example, with regard to FIG. 12, test procedures can be mapped to requirements 1206, as requirements are mapped to regulations 1210. In addition, test procedures can be added and/or edited as discussed, for example, with regard to FIGs. 14-16. At step 2106, testing is conducted, and test results are recorded as discussed, for example, with regard to FIG. 15.

At step 2108, the test results for one or more requirements associated with a requirements category (as will be discussed herein) are reviewed and, at decision step 2110, a determination is made if any requirements have not been satisfied.

If there are no requirement failures, then at step 2112 the risk is deemed
negligible. As determined at decision step 2116, additional risk categories are reviewed at step 2108.

If at decision step 2110 it is determined that any requirements have failed, the risk for category n is calculated based on a predetermined risk formula (an exemplary risk formula will be discussed herein).

After a determination is made at decision step 2116 that no requirement categories remain (i.e., all requirement categories have been reviewed for failure of one or more associated requirements), at step 2118 the system risk is calculated based on a predetermined system risk formula (an exemplary system risk formula will be discussed herein).

\[ \text{a) Generate Threat String of Requirement Category (step 2202)} \]

FIG. 22 is an exemplary flow diagram of a risk assessment method contemplated by at least some embodiments of the present invention. As shown in FIG. 22, at step 2202, at least some embodiments of the present invention generate a threat string for a requirement category. As used herein, a requirement category is a category that can be used to contain one or more related requirements. Exemplary names for requirement categories are as follows:

- Encryption
- Network Perimeter Security
- Key Management, Physical Communications Link Security/PDS
- Routing and Switching
- Wireless Communication Security
- Access Control
- Antivirus Protection
- Audit, Identification and Authentication / Password / Trusted Path
- Security Marking and Printing
- Mobile Code
- Object Reuse
- Screen Saver
- Ports and Services
- System Configuration
- System and Data Integrity
- Security Warning Banner
Security Testing
Emanation Security
Equipment Maintenance
Equipment Ownership
5
Firmware Configuration
Hardware Configuration
Equipment and Media Marking
Media Handling and Destruction / Purging
Portable Equipment
Personnel Clearances / Screening
Personnel Designations
Foreign Nationals
Maintenance Personnel
Physical Access Control
10
Environmental Security
Equipment Security
Facility Security
Assessment / Assurance
Configuration Management
Contingency Planning
Copyright, Documentation (Development)
Documentation (Operational)
Email/Web/Internet Policy
Incident Reporting
20
Tactical Systems
Penetration / Firewall
Security Awareness Training.

Other requirements categories can be used in lieu of or in addition to those enumerated above.

For each requirement utilized in the project, the threat string of the requirement is a score for each of the generic threat elements (e.g., fire, flood, hardware, power, software design error, etc.). In one or more embodiments of the present invention, each element of the threat string indicates a respective potential of a given threat element to
exploit a vulnerability caused by failure of one or more requirements associated with a requirements category.

In at least some embodiments, the user performing the C&A is presented with a series of questions pertaining to the environment for which the C&A will be performed. (This information could also be obtained in an automated fashion using any number of known techniques). An estimate of the threat level can then be rendered based on the operators’ answers. In one or more embodiments of the present invention, a user can optionally change any of the system determined threat element scores. Exemplary values for generic threat elements are as follows:

<table>
<thead>
<tr>
<th>Threat Element Score</th>
<th>Interpretation</th>
</tr>
</thead>
<tbody>
<tr>
<td>N</td>
<td>Threat element is not applicable to this requirement category or has negligible likelihood of occurrence</td>
</tr>
<tr>
<td>L</td>
<td>Threat element has low likelihood of occurrence for this requirement category</td>
</tr>
<tr>
<td>M-L</td>
<td>Threat element has medium-low likelihood of occurrence for this requirement category</td>
</tr>
<tr>
<td>M</td>
<td>Threat element has medium likelihood of occurrence for this requirement category</td>
</tr>
<tr>
<td>M-H</td>
<td>Threat element has medium-high likelihood of occurrence for this requirement category</td>
</tr>
<tr>
<td>H</td>
<td>Threat element has high likelihood of occurrence for this requirement category</td>
</tr>
</tbody>
</table>

For example, for one requirement category, generic threat elements 1-29, as defined in FIG. 23, may have a project threat profile as follows:

M-LHNLMLLM-HMMMLMLLMMLMLMLMLLMLLNN

corresponding, respectively, to elements 1-29. For this project threat profile, the potential of a threat to exploit a vulnerability associated with (or caused by) flooding is thus considered high. Similarly, each requirement category used for the project C&A can have a different threat string associated therewith.

FIG. 24 shows an exemplary screen display that enables a user to view the
setting for the Antivirus Protection requirements category, which shows a default level of risk for each threat element (or threat) shown in FIG. 23. In accordance with one or more embodiments of the present invention, the user can also adjust the system 200 provided default values by using, for example, a pulldown menu associated with each threat element. Exemplary pulldown menu choices are negligible, low, medium-low, medium, medium-high or high, although they could also be, for example, numerical in nature. Note that in these embodiments of FIG. 24 that Threat Group column 2302 corresponds to at least one of columns 2302a, 2302b, 2302c of FIG. 23. Similarly, Weight column 2402 of FIG. 24 corresponds to the threat element scores, as discussed with regard to FIG. 23.

b) Generate Threat/Susceptibility String of Project (step 2204)

In step 2204, a threat string (which can also be referred to as a susceptibility string, corresponding to column 2504 of FIG. 25A) is generated for the project. Specifically, in one or more embodiments of the present invention, upon completion of steps 100, 102 and 104, the system can generate a threat string (based upon, for example, user answers as shown, for example, in FIG. 13), with each character in the string representing one of the generic threat elements in the same order as they exist in the threat string of the requirement categories as shown, for example, in FIG. 23. A user can also override any system determined threat string values. Each element in the threat string generally represents how susceptible the project as a whole is to each threat element. More generally, in one or more embodiments, the threat string can generally represent the presence of the threat, the likelihood of occurrence of the threat, and/or the potential damage caused by the threat (when it is present). An exemplary scoring system is as follows:

<table>
<thead>
<tr>
<th>Threat String of Project</th>
<th>Interpretation</th>
</tr>
</thead>
<tbody>
<tr>
<td>N</td>
<td>The project is not susceptible to this threat element (or has a negligible susceptibility to this threat element)</td>
</tr>
<tr>
<td>L</td>
<td>The project has a low susceptibility to this threat element</td>
</tr>
<tr>
<td>M-L</td>
<td>The project has a medium-low susceptibility to this threat element</td>
</tr>
<tr>
<td>M</td>
<td>The project has a medium susceptibility to this threat element</td>
</tr>
<tr>
<td>-----</td>
<td>-------------------------------------------------------------</td>
</tr>
<tr>
<td>M-H</td>
<td>The project has a medium-high susceptibility to this threat element</td>
</tr>
<tr>
<td>H</td>
<td>The project has a medium susceptibility to this threat element</td>
</tr>
</tbody>
</table>

Thus, for example, if the system being tested is highly vulnerable to Floods, the character in the threat correlation string corresponding to Floods would contain a score of “H.”

c) Determine Risk Profile for Each Requirement Category (step 2206)

As indicated at step 2206, the risk profile for each requirement category is determined. Specifically, for each requirement category, the threat string of the requirement category (as determined at step 2202) is applied against the threat string of the project (as determined at step 2204).

For example, the threat string of a requirement category (e.g., encryption) may have the following threat string (as determined at step 2202, and shown in column 2502 of FIG. 25A):

M-LHNLLLMM-HMMMLLLMMMLLLMLLLLNN

and the threat string of the project (as determined at step 2204, and shown in column 2504 of FIG. 25A) may be:

HHNM-LHLMM-HNHHMLNNLMLHNNLHNLHLMH

In this case, in accordance with an exemplary process according to at least some embodiments of the present invention, the combined risk profile string as determined in accordance with FIG. 25A would be:

M-HHNLMMLM-LMMLMMMLLLNMLMLMLMLMLNN

The above string was derived by comparing the threat string of the requirements category (corresponding to column 2502) with the threat string of the project (corresponding to column 2504), and determining the resulting threat string in accordance with column 2506. For example, a medium level of risk for the requirements category (corresponding to column 2502) and a negligible level of risk for the project (corresponding to column 2504) yields a negligible level or risk
(corresponding to column 2506) to the target system for that threat element.

More particularly, and using the Antivirus Subgroup* (requirements category) 2404 shown in FIG. 24 as an example, the negligible weight in Humidity indicates that Humidity has a negligible potential to exploit Antivirus protection. Suppose, however that the system as a whole has a high degree of exposure to humidity. In accordance with FIG. 25A, the low value associated with column 2502 in combination with the high value associated with column 2504 yields a composite threat (shown in column 2506) of medium.

The respective threat strings for each requirements category used for a particular C&A are similarly determined. Initially, the highest risk level in the combined string for a given requirements category is preferably used as the risk level for that requirements category. Thus, for the combined string above, the risk level of the requirements category is high, since there is an H in the second position. Similarly, if M were the highest risk level that appears in a combined string, then the risk level for a failure of that test procedure would be medium, etc. Similarly, for an initial system risk, the highest level of risk in any requirements category can be used as a baseline system risk.

In one or more embodiments of the present invention, the initial risk level of a requirement category can be (but is not necessarily) adjusted based upon the percentage of failed requirements in a requirements category. Specifically, each requirements category can have \( n \) requirements associated therewith, and each requirement can have one or more associated test procedures. The initial risk level of a requirement category can then be adjusted based upon, for example, the table shown in FIG. 25B.

Suppose, for example, that 10% of requirements failed in a particular requirements category. According to row 2508 of FIG. 25B, the importance value is equal to (or set to) 1. FIG. 25C is then utilized to adjust the risk of the requirements category based upon the importance value. In this particular instance, row 2510 indicates that the adjusted risk value is \(-2\). Therefore, the risk level of the requirements category would be reduced by two levels (from high to medium-high, and then from medium-high to medium) to provide a resulting requirements category risk level of medium.

Similarly, suppose that the highest threat level resulting from FIG. 25A is
medium, and the 62% of the requirements within that requirements category have failed. Then, in accordance with FIG. 25B, the importance value is 4. In accordance with FIG. 25A, the adjusted risk level is one. Thus, the risk level of the requirements category would be adjusted up (from medium) to medium-high. Other combinations of the use of FIGs. 25A, 25B and 25C are clearly possible. As shown in FIGs. 25B and 25C, when the importance value of FIG. 25B is 3, the initial risk level of a requirement category remains the same (i.e., is not adjusted, as indicated by the corresponding adjusted risk value shown in FIG. 25C).

d) Determine Overall System Level Risk (step 2208)

In addition to the individual risk level scores for each requirements category as determined in step 2206, an overall risk level for the project is also determined as indicated by step 2208. As shown in FIG. 26, in one or more embodiments of the present invention, the overall system risk level is defined as the highest risk value among those found in any of one or more requirements categories. The overall system risk can also be determined by comparing the results of one or more physical sites or subsystems.

Thus, if it is determined that any requirements category has a “high” risk (as indicated by decision step 2602), then the overall risk for the system is high as indicated by a step 2604. If any requirements category has a “medium-high” risk (as indicated by decision step 2606), then the overall risk for the system is medium-high as indicated by step 2608. If any requirements category has a “medium” risk (as indicated by decision step 2610), then the overall risk for the system is medium as indicated by step 2612. If any requirements category has a “medium-low” risk (as indicated by decision step 2614), then the overall risk for the system is medium-low as indicated by step 2616. If any requirements category has a “low” risk (as indicated by decision step 2618), then the overall risk for the system is low as indicated by step 2620. Finally, if the risk of all (of one or more) requirements categories is “negligible,” then the overall risk for the system is negligible, as indicated by step 2622. The user also can have the ability to override the overall system risk level as determined in accordance with the above methodology. In such a case, the user may also provide explanatory text to accompany the overall user-defined system risk level.
Publishing

In the publishing step 110, one or more embodiments of the present invention collate the results of the certification process, and generate a documentation package that can be used for accreditation. The information gathered during activities associated with and/or corresponding to steps 100, 102, 104, 106, and 108, can be reformatted by, for example, organizing it into appropriate documents, document subsections or subparagraphs, sections and/or appendices, etc.

As shown in FIG. 27, one or more embodiments of the present invention allow a user to print a complete project report as indicated at 2702. An embodiment of a complete project report includes elements 2704a-2724a, as indicated by the corresponding checked boxes for each element in FIG. 27. In one or more embodiments contemplated by the present invention, a user can select additional screen displays (not shown) by activating one or more of menu elements 2704b-2724b (each respectively corresponding to elements 2704a-2724a). Any or all of elements 2704a-2724a can be generated by clicking, for example, the desired boxes corresponding to reports 2704a-2724a, and clicking Generate .pdf button 2726.

When a user selects any or all of elements 2704a-2724a, a report is provided that complies with, for example, the DITSCAP (DoD Instruction 5200.40). It is also contemplated that accreditation can be automated, so that no accreditation agency is needed. In such an embodiment, when sufficient test related results and/or information is provided to the system 200, a method according to the present invention can automatically determine that accreditation requirements have been satisfied.

Workflow Manager

The present invention also provides a "front end" (called Workflow Manager (WFM)) that adds workflow functionality to the C&A process. By using the WFM, tasks (a unit of work) can be defined. Each task can, for example, be opened, submitted, and approved by a user (e.g., an analyst). When an event of interest takes place, an e-mail or other electronic notification can be sent to the appropriate user(s). The present invention thus provides an e-mail notification setup graphical user interface (GUI) that enables users to define and enter, for example, Role/Title, Users, and task notifications in support of the e-mail notification functionality.

In accordance with at least some embodiments, the WFM of the present
invention provides, for example, electronic control and authorization of access to
documents, notification of designated individuals when a predefined event occurs,
document approval, tracking, status reporting, and/or tracking of document revisions.
The WFM also advantageously provides for the revision, approval, and release of
documents in a collaborative environment. In addition, the WFM also can help ensure
that published content (e.g., a C&A report or portion thereof) is accurate and timely,
providing for the automated document release and/or user notification for time-
sensitive documents or content.

The WFM enables users to define tasks (units of work) that resemble or
correspond to an organization's best practices. WFM provides a GUI that can be used
to notify users when the state of a task changes.

The following terms and associated definitions associated with the WFM are
provided:

**Process Step (PS):** A unit of work that normally corresponds, for example, to a
screen display.

**Task:** A unit of work within WFM that consists, for example, of one or more
PSs.

**Project:** A set of tasks that can be used for a particular C&A.

**Submittal:** When work is completed on a task, an analyst with appropriate
permission can submit it for approval. Submittal can also optionally lock the
information in the task so no further change can take place.

**Approval:** An analyst with appropriate permission can approve a submitted task.
In accordance with at least some embodiments of the present invention,
when a task is approved, its content preferably remains locked. Subsequent
tasks may then become available for work.

**Disapproval:** An analyst with appropriate permission can disapprove a
submitted task. In accordance with at least some embodiments of the present
invention, when a task is disapproved, its content is unlocked so that further
work may be done to complete it.

**Prerequisite**: Tasks within a Project can be set up with dependencies. In accordance with at least some embodiments of the present invention, any given task may be configured so that it only becomes available for work when certain prerequisite task have been approved.

**Reopening**: An analyst with appropriate permission can reopen an already-approved task if new information has become available and the task must be revised. In accordance with at least some embodiments of the present invention, reopening preferably unlocks the information in the task so that it may be revised. Subsequent tasks with dependencies may once again become unavailable for work.

FIG. 28 is an exemplary screen display that enables the React component of the present invention to be utilized in the C&A for a project. As discussed with regard to FIG. 2, react module 204 can inform, for example, affected users when pre-specified and/or predetermined events occur.

React module 204 can be activated by selecting React in Component: field 2802, and indicating that the React Engine: is enabled in field 2804. Work Engine: field 2806 enables, for example, a commercially available external workflow product to be integrated with a C&A project. Email server: field 2810 can be used to indicate the name of the e-mail server that will provide the workflow events. Email from: field 2810 can be used to indicate the e-mail account the will deliver the workflow events.

Finally, Polling Interval: field 2812 can be used to specify the time interval at which the email server specified in field 2808 will be polled for workflow events.

FIG. 29 is an exemplary Project Management display. By clicking on Add Project/Template button 2918, a project can be added, such as found under Project Name column 2908. A project can be opened by clicking on an Open icon, under column 2902, associated with (or corresponding to) a project. Status column 2904 indicates whether the current project is active or inactive. Type column 2906 refers to either a template (that can be used to create a project), or an actual project.
Subscription Expiration column 2910 refers to the date that the software subscription expires (as can be determined by, for example, Subscription Key 630). By clicking on an icon under Properties column 2914, the user will be taken to an exemplary screen such as shown in FIG. 30 indicating properties of the project.

With regard to FIG. 30, a user can enter appropriate descriptive information in Project Name* field 3002 and Description* field 3004. In one embodiment of the present invention, and as discussed with regard to FIG. 6, users can also be provided (by, for example, the assignor and/or licensor of the present invention) a key to enter in Subscription Key* field 3006 which can be used, for example, to identify an organization. Status* field 3007 can be used to designate whether the project is Active or Inactive. In accordance with at least some embodiments of the present invention, users can access at least a portion of one or more active projects (e.g., one or more PSs) to which they have been granted user rights. When a project is inactive, user are not granted access rights. A system administrator, however, could change the status of the project from inactive to active, in which case users will have access to the project in accordance with their user rights.

At Available as a Template* 3008, a user can allow (by clicking the Yes button) the current project template to be used as a baseline for other templates or projects. Note that the DITSCAP Classic Project Template project name appears at 3020 when the Yes button is activated. At File to Restore From: field 3010, a user can optionally specify a backup file location.

The user can select the Reset button 3012 to reset the screen display to its default condition. Clicking Cancel button 3018 will return the user to, for example, the previous screen. If the user selects the Save button 3010, the user can save the current settings, and optionally be advanced to, for example, a subsequent screen.

When a user clicks Assign Users 2912, an exemplary screen such as shown in FIG. 31 is presented. A users login name can be displayed under Login column 3102. Similarly, a users first name can be displayed under First Name column 3108, and a users email address can be displayed under Email column 3110. The type of the user can also be displayed under Type column 3104. A box under Admin column 3112 can be checked to indicate that the user has administrative privileges. Finally, by using, for example a pulldown menu under Role column 3114, a user can be assigned a role,
which can be further defined by an exemplary screen display such as shown in FIG. 32.

FIG. 32 can be used to enable a user to enter information identifying all the project personnel associated with the accreditation effort. The personnel are preferably identified by the role, as discussed below, that they serve in the accreditation process.

At least one entry for each role is preferably defined for the project.

For example, the following role names can be provided in Role Name column 3202 by, for example, clicking on Add Role button 3204. A Role Name can generally be considered to be the role associated with the accreditation team member. The available choices can include:

Accreditation Team Lead 3206 - The person in charge of the accreditation effort, usually the Project Manager.

Accreditation Team Member 3208 - All the members of the accreditation team (analysts, testers, etc.).

Certification Authority 3210 - Person in charge of the system certification.

Certification Authority POC 3212 - Point of Contact (POC) to the CA.

DAA 3214 - Designated Approving Authority. Person ultimately responsible for the accreditation of the system.

DAA POC 3216 - Point of Contact (POC) to the DAA.

ISSO 3220 - Information System Security Officer. Person responsible for the security implementation of the system being accredited.

Lead Tester 3222 – The head tester (in charge of a team or group of testers).

Program Manager 3226 - Program manager of the system being accredited.

User Representative 3228 - Representative from the user community.

By clicking on Add Role button 3204, a user can be taken to a screen display such as shown in FIG. 33, where a Role Name can be added in field 3302. A user can also optionally add a description of the role in Description field 3304. Activating an icon under Properties column 3206 will also take a user to a screen similar to that shown in FIG. 33.

In addition, project access can also be defined. For each Task Name 3305
(e.g., Content Management, Information Gathering, etc.), an administrator, for example, can determine the extent to which the user can determine whether other users associated with the project have access to a particular task. For example, when an administrator activates a button 3307 (so that it contains a bullet, such as shown at 3307) under column 3306 that is associated with a particular task, users associated with a task having an activated button are not granted access to the project. When one or more activation buttons associated with column 3308 are activated, users associated with a task are granted read only privileges for aspects of the project whose respective access buttons are activated. When an activation button under column 3310 is activated, users have full access (e.g., read and write access) for materials (e.g., screen displays) associated with a given task.

In addition, access rights can be specified with regard to whether a user can Reopen 3312, Submit 3314, Approve 3316, and/or Disapprove 3318 one or more designated task names. For example, if box 3311 is activated (e.g., a user can click on the box, and an “X” can appear therein), the user(s) associated with the Content Management task can reopen aspects of the project associated therewith.

In addition, a user can also set notification parameters for each Task Name 3305. When a user clicks on a box (e.g., 3319) associated with a particular task under column 3320, users will be notified when a corresponding task is reopened (by another user). For example, if a user activates box 3319, users associated with the Content Management task will be notified each time that the Content Management task is reopened. Similarly, one or more boxes under each of columns 3322, 3324, and 3326 can be activated so that user are respectively notified when corresponding tasks are submitted, approved and disapproved.

The user can save the results by activating (e.g., clicking on) Save button 3328. Activating Reset button 3330 will reset the screen to its default condition. Activating Cancel button 3332 can return the user to, for example, a previous screen.

FIG. 34 is an exemplary screen display that enables a user to enter a Task Name* 3404 and associated Description.: The Available Process Steps: are shown in window 3406, from which the user can select which process steps he wishes to associate with the Task Name* 3404. The Selected: process steps are shown in window 3408. The user can add process steps via window 3406 one at a time by
selecting button 3414, or add all available process steps by selecting button 3418.
Selected process steps can similarly be removed from window 3408 by clicking buttons
3416 and 3420, respectively.

The user can also select one or more tasks displayed in Work Tasks Available
As Prerequisite: 3410 window. When selected, such task(s) must be completed before
the Tasks entered at 3404 can begin. One or more prerequisite tasks individually can be
added via button 3422, whereas all prerequisite tasks can simultaneously be added via
button 3426. Prerequisite tasks can be similarly removed by selecting buttons 3424 and
3428, respectively. Selections can be saved by selecting button 3430, canceled by
selecting button 3432, and reset by selecting button 3434. Selecting Cancel button
3432 can, for example, return the user to the previous screen, whereas selecting Reset
button 3434 can reset FIG. 34 to its default.

FIG. 35 is an exemplary screen display that shows Project Personnel. At column
3504, each user’s Name can be provided. At column 3506, the Role of the user is
indicated. At column 3508, the user’s Organization can be provided (e.g., Tier I or
Tier II). In the event that Tier II is specified for the organization, the Office 3510 can
be provided at column 3510. By clicking on Properties 3512, the user can be taken to
an exemplary screen display that enables at least some of the following information
pertaining to a particular user to be entered: Role Name (e.g, Accreditation Team
Member), Title (e.g., Mr., Ms.), First Name, Middle Initial, Last Name, Office
(corresponding to column 3510), Street Address, Zip Code, Telephone number,
Facsimile number, and e-mail address. By clicking an icon as shown in Copy column
3514, a particular user’s profile will be copied (to avoid having to manually reenter at
least some information). Finally, at column 3516, a Delete icon can be activated to
delete a particular user from the project.

FIG. 36 is an exemplary flow diagram of the Workflow Manager process. At
decision step 3602, the user determines whether to add a project. A screen display such
as shown, for example, in FIG. 30 can be used to add a project. If a project is not to be
added, the process ends 3624. If the user decides to add a project, at decision step 3604
the user determines whether to base the new project based on an existing project. If the
user bases the new project on an existing project, the user selects an existing project at
step 3606 (by, for example, using the Available Templates: menu shown in FIG. 30).
If the user does not base the new project on an existing project, the user types in information to define the project (as discussed with regard to FIG. 30).

At step 3610, the user adds one or more process steps to a task (e.g., Information Gathering, as shown in FIG. 34) and, at decision step 3612, determines whether there will be any prerequisite process steps before beginning another task. If, as discussed, for example, with regard to FIG. 34, there are prerequisite steps, the user adds the prerequisite steps at step 3614. If there are no prerequisite steps, or after step 3614, the user adds roles associated with the project (as discussed, for example, with regard to FIGs. 32-33). At step 3618, a role is assigned to each user (as discussed, for example, with regard to FIGs. 31 and 35). At decision step 3620, a system administrator, for example, can determine whether any user(s) should be notified upon, for example, the opening, completion, or commencement of a task (as discussed with regard to FIG. 33). If it is determined that any user(s) should be notified, the administrator sets user notification(s) (as discussed, for example, with regard to columns 3320, 3322, 3324 and 3326 of FIG. 33). If no user notification is required, or after user notification is set at step 3622, the process ends at step 3624.

Computer Implementation

The techniques of the present invention may be implemented on a computing unit such as that depicted in FIG. 37. In this regard, FIG. 37 is an illustration of a computer system which is also capable of implementing some or all of the computer processing in accordance with computer implemented embodiments of the present invention. The procedures described herein are presented in terms of program procedures executed on, for example, a computer or network of computers (as shown, for example, in FIG. 40).

Viewed externally, in FIG. 37, a computer system designated by reference numeral 3700 has a computer portion 3702 having disk drives 3704 and 3706. Disk drive indications 3704 and 3706 are merely symbolic of a number of disk drives which might be accommodated by the computer system. Typically, these could include a floppy disk drive 3704, a hard disk drive (not shown externally) and a CD ROM indicated by slot 3706. The number and type of drives vary, typically with different computer configurations. Disk drives 3704 and 3706 are in fact optional, and for space considerations, are easily omitted from the computer system used in conjunction with
the production process/apparatus described herein.

The computer system 3700 also has an optional display 3708 upon which information, such as the screens illustrated in, for example, FIGs. 4-10, etc. may be displayed. In some situations, a keyboard 3710 and a mouse 3712 are provided as input devices through which input may be provided, thus allowing input to interface with the central processing unit 3702. Then again, for enhanced portability, the keyboard 3710 is either a limited function keyboard or omitted in its entirety. In addition, mouse 3712 optionally is a touch pad control device, or a track ball device, or even omitted in its entirety as well, and similarly may be used as an input device. In addition, the computer system 3700 may also optionally include at least one infrared (or radio) transmitter and/or infrared (or radio) receiver for either transmitting and/or receiving infrared signals.

Although computer system 3700 is illustrated having a single processor, a single hard disk drive and a single local memory, the system 3700 is optionally suitably equipped with any multitude or combination of processors or storage devices. Computer system 3700 is, in point of fact, able to be replaced by, or combined with, any suitable processing system operative in accordance with the principles of the present invention, including hand-held, laptop/notebook, mini, mainframe and super computers, as well as processing system network combinations of the same.

FIG. 38 illustrates a block diagram of the internal hardware of the computer system 3700 of FIG. 37. A bus 3802 serves as the main information highway interconnecting the other components of the computer system 3700. CPU 3804 is the central processing unit of the system, performing calculations and logic operations required to execute a program. Read only memory (ROM) 3806 and random access memory (RAM) 3808 constitute the main memory of the computer 3702. Disk controller 3810 interfaces one or more disk drives to the system bus 3802. These disk drives are, for example, floppy disk drive 3704 or CD ROM 3706. As indicated previously, these various disk drives and disk controllers are optional devices.

A display interface 3818 interfaces display 3708 and permits information from the bus 3802 to be displayed on the display 3708. Again as indicated, display 3708 is also an optional accessory. For example, display 3708 could be substituted or omitted. Communications with external devices, for example, the other components of the
system described herein, occur utilizing communication port 3816. For example, optical fibers and/or electrical cables and/or conductors and/or optical communication (e.g., infrared, and the like) and/or wireless communication (e.g., radio frequency (RF), and the like) can be used as the transport medium between the external devices and communication port 3816. Peripheral interface 3820 interfaces the keyboard 3710 and the mouse 3712, permitting input data to be transmitted to the bus 3802.

In alternate embodiments, the above-identified CPU 3804, may be replaced by or combined with any other suitable processing circuits, including programmable logic devices, such as PALs (programmable array logic) and PLAs (programmable logic arrays). DSPs (digital signal processors), FPGAs (field programmable gate arrays), ASICs (application specific integrated circuits), VLSIs (very large scale integrated circuits) or the like.

One of the implementations of the invention is as sets of instructions resident in the random access memory 3808 of one or more computer systems 3700 configured generally as described above. Until required by the computer system, the set of instructions may be stored in another computer readable memory, for example, in the hard disk drive 3812, or in a removable memory such as an optical disk for eventual use in the CD-ROM 3706 or in a floppy disk (e.g., floppy disk 3902 of FIG. 39) for eventual use in a floppy disk drive 3704. Further, the set of instructions (such as those written in Java, HyperText Markup Language (HTML), Extensible Markup Language (XML), Standard Generalized Markup Language (SGML), and/or Structured Query Language (SQL)) can be stored in the memory of another computer and transmitted via a transmission medium such as a local area network or a wide area network such as the Internet when desired by the user. One skilled in the art knows that storage or transmission of the computer program medium changes the medium electrically, magnetically, or chemically so that the medium carries computer readable information.

Databases utilized in conjunction with the present invention can be implemented using, for example, Oracle, Microsoft Structured Query Language (MS SQL) Server, MS Jet Engine (Access), or a database management system that has Java Database Connectivity (JDBC) support. For presentation (e.g., screen displays), the present invention can be implemented in JavaServer Pages (JSP), which can be rendered into HTML. Classes and/or modules can generally be written in
JAVA. Detect module 222 can also utilize a few C++ classes and modules. Exported
data (e.g., archives, snapshots, backups, publishing streams, etc.) can be implemented
using extensible Markup Language (XML) format. A web server utilized in conjunction
with the present invention can be implemented using, for example, Microsoft IIS or
Apache. Finally, Catalina (also known as Tomcat) can be used to implement Java
Servlet and JSP technologies.

FIG. 40 is an exemplary network implementation of the present invention. As
shown, one or more computer systems 3700 can be operationally connected to a
network 4002 such the Internet, a LAN, WAN, or the like. The network
implementation of the present invention enables two or more users to collaboratively
work, via the network 4002, on one or more C&As. The computer portion 3702a
comprises a WEB C&A component 4002 (generally corresponding, for example to
FIGs. 1-27) and a Workflow Manager (WFM) component 4005 (generally
corresponding, for example, to FIGs. 28-35). WEB C&A component 4002 and WFM
component 4004 are shown separately to indicate that the WFM is an optional aspect of
the WEB C&A component, and is not required for the operation thereof.

FIG. 41 is an entity relationship diagram (ERD) that describes the attributes of
entities and the relationships among them, and illustrates the basic data abstraction of
an embodiment of the system. FIGs. 41a-d show FIG. 41 in expanded form. As known
to those skilled in the art, an ERD is a conceptual representation of real world objects
and the relationships between them. It defines information that the systems create,
maintain, process, and delete, as well as the inherent relationships that are supported by
the database (i.e., data store).

At least some embodiments of the present invention can utilize a relational
database to store and organize all information such as, for example, test procedures,
standards/regulations, and user entered information. The design of an embodiment of
the database is provided in the ERD shown in FIG. 41. The database is initially
populated with security requirements, test procedures and related information to
facilitate the operation of the system. As information is entered by the user and
calculated by the system, it is also recorded in the database. At least some embodiments
of the present invention produce output documentation that can be formatted in
accordance with, for example, DITSCAP and/or NIACAP standard(s).
The ERD shown in FIG. 41 uses conventional notation. Each entity, as shown in FIG. 41, comprises a rectangular box. A many-to-many (N:M) relationship shows that each occurrence of entity A is related to one or more occurrences of entity B, and each occurrence of entity B is related to one or more occurrences of entity A.

The many features and advantages of the invention are apparent from the detailed specification, and thus, it is intended by the appended claims to cover all such features and advantages of the invention which fall within the true spirit and scope of the invention. Further, since numerous modifications and variations will readily occur to those skilled in the art, it is not desired to limit the invention to the exact construction and operation illustrated and described, and accordingly, all suitable modifications and equivalents may be resorted to, falling within the scope of the invention. While the foregoing invention has been described in detail by way of illustration and example of preferred embodiments, numerous modifications, substitutions, and alterations are possible without departing from the scope of the invention defined in the following claims.
CLAIMS

Having thus described our invention, what we claim as new and desire to secure by Letters Patent is as follows:

1. A computer-implemented method of enabling a user to assess the risk of and/or determine the suitability of a target system to comply with at least one predefined standard, regulation and/or requirement, the target system including hardware and/or software, the method comprising the steps of:
   a) receiving at the computer at least one of a newly encountered hardware, software and/or operating system threat;
   b) updating a requirements repository to account for the threat;
   c) updating one or more target system test procedures to account for the threat; and
   d) conducting a risk assessment of the target system.

2. The method according to claim 1, further comprising the step of determining, by the computer, at least one of target system hardware, software and operating system components.

3. The method according to claim 2, further comprising the step of conducting a further risk assessment subsequent to said determining step.

4. The method according to claim 1, wherein at least one of the updates in said steps b) and c) is electronically transmitted to the computer.

5. The method according to claim 1, further comprising the step of verifying that said computer is authorized to receive the electronic transmission.

6. A system for enabling a user to select at least one of a plurality of predefined process steps to create a tailored sequence of process steps that can be used to assess the risk of and/or determine the suitability of a target system to comply with at least one predefined standard, regulation and/or requirement, the target system including hardware and/or software, the computing system comprising:
a) means for receiving at the computer at least one of a newly encountered hardware, software and operating system threat;

b) means for updating a requirements repository to account for the threat;

c) means for updating one or more target system test procedures to account for the threat; and

d) means for conducting a risk assessment of the target system.

7. The system according to claim 6, wherein said conducting means determines at least one of target system hardware, software and operating system components.

8. The system according to claim 7, wherein said conducting means conducts a further risk assessment subsequent to determining at least one of target system hardware, software and operating system components.

9. The system according to claim 6, wherein at least one of the updates is electronically transmitted to the computer.

10. The system according to claim 6, further comprising means for verifying that said computer is authorized to receive the electronic transmission.

11. A computer program product residing on a computer readable medium, for enabling a user to assess the risk of and/or determine the suitability of a target system to comply with at least one predefined standard, regulation and/or requirement, the target system including hardware and software, the computer program product comprising instructions for causing the computer system to interact with a user and enabling at least one of the computing system and the user to perform the steps of:

a) receiving at the computer at least one of a newly encountered hardware, software and/or operating system threat;

b) updating a requirements repository to account for the threat;

c) updating one or more target system test procedures to account for the threat; and

d) conducting a risk assessment of the target system.
12. The computer program product according to claim 11, further comprising instructions for determining, by the computer, at least one of target system hardware, software and operating system components.

13. The computer program product according to claim 12, further comprising instructions for conducting a further risk assessment subsequent to said determining step.

14. The computer program product according to claim 11, wherein at least one of the updates in said steps b) and c) is electronically transmitted to the computer.

15. The computer program product according to claim 11, further comprising instructions for verifying that the computing system is authorized to receive the electronic transmission.

16. A method of updating a data repository of a system that enables a user to assess the risk of and/or determine the suitability of a target system to comply with at least one predefined standard, regulation and/or requirement, the target system including hardware and software, the method comprising the steps of:

   a) collecting data pertaining to at least one of a newly encountered hardware, software and operating system threat;

   b) formatting the data to be compatible with a data repository associated with the computer; and

   c) at least one of generating and updating a test procedure associated with the at least one predefined standard, regulation and/or requirement.

17. The method according to claim 16, further comprising the step of transmitting to the computer at least one of the formatted data and the formatted test procedure to the computer.
18. The method according to claim 16, further comprising the step of determining, by the computer, at least one of target system hardware, software and operating system components.

19. A system for updating a data repository of a system that enables a user to assess the risk of and/or determine the suitability of a target system to comply with at least one predefined standard, regulation and/or requirement, the target system including hardware and software, the system comprising:
   a) means for collecting data pertaining to at least one of a newly encountered hardware, software and operating system threat;
   b) means for formatting the data to be compatible with a data repository associated with the computer; and
   c) means for at least one of generating and updating a test procedure associated with the at least one predefined standard, regulation and/or requirement.

20. The system according to claim 19, further comprising means for formatting the test procedure to be compatible with a data repository associated with the computer.

21. The system according to claim 19, further comprising means for transmitting to the computer at least one of the formatted data and the formatted test procedure to the computer.
1/48

GATHER SYSTEM CONFIGURATION INFORMATION  100

DETERMINE/SELECT REQUIREMENTS  102

SELECT TEST PROCEDURES  104

CONTENT MANAGEMENT  106

RISK ASSESSMENT  108

PRINT DOCUMENTATION  110

FIG. 1
<table>
<thead>
<tr>
<th>SELECT</th>
<th>502</th>
<th>504</th>
<th>506</th>
<th>CHANGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALL</td>
<td>NAME</td>
<td>DESCRIPTION</td>
<td>STATE</td>
<td>STATE</td>
</tr>
<tr>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>☐     1. CONTENT MANAGEMENT</td>
<td>CONTENT MANAGEMENT</td>
<td>OPEN</td>
<td>→</td>
<td></td>
</tr>
<tr>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>☐     2. INFORMATION GATHERING</td>
<td>INFORMATION GATHERING</td>
<td>OPEN</td>
<td>→</td>
<td></td>
</tr>
<tr>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>☐     3. REQUIREMENTS ANALYSIS</td>
<td>REQUIREMENTS ANALYSIS</td>
<td>OPEN</td>
<td>→</td>
<td></td>
</tr>
<tr>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>☐     4. TESTING</td>
<td>TESTING</td>
<td>OPEN</td>
<td>→</td>
<td></td>
</tr>
<tr>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>☐     5. RISK ASSESSMENT</td>
<td>RISK ASSESSMENT</td>
<td>OPEN</td>
<td>→</td>
<td></td>
</tr>
<tr>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>☐     6. PUBLISHING</td>
<td>PUBLISHING</td>
<td>OPEN</td>
<td>→</td>
<td></td>
</tr>
</tbody>
</table>

FIG. 5A
<table>
<thead>
<tr>
<th>HOME</th>
<th>RESOURCES</th>
<th>PREFERENCES</th>
<th>XACTA ADVISOR</th>
<th>SUPPORT</th>
</tr>
</thead>
<tbody>
<tr>
<td>BACK TO...</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TIER I ADMINISTRATION</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TIER II</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TIER II ACME CORPORATION</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CONTINUOUS ASSESSMENT</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CONTINUOUS ASSESSMENT</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DETECT CONFIGURATION</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SCANNER CONSTRAINTS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**SCANNER CONSTRAINTS**

**PROCESSING WINDOW** 802

**VULNERABILITY FAMILY SCAN CONSTRAINTS (CHECK TO ENABLE)**

- BACKDOORS: ☑
- CGI ABUSES: ☑
- CISCO: ☑
- CRASHES AN IIS FTP SERVER: ☑
- DENIAL OF SERVICE: ☑
- FTP: ☑
- FIND WHAT IS LISTENING ON WHICH PORT: ☑
- FINGER ABUSES: ☑
- FIREWALLS: ☑
- GAIN A SHELL REMOTELY: ☑
- GAIN ROOT REMOTELY: ☑
- GENERAL: ☑
- MISC: ☑
- NIS: ☑
- PORT SCANNERS: ☑
- RPC: ☑
- REMOTE FILE ACCESS: ☑
- SMTP PROBLEMS: ☑
- SNMP: ☑
- SETTINGS: ☑
- TURNS THE REMOTE SWITCH INTO A HUB: ☑
- UNTESTED: ☑
- USELESS SERVICES: ☑
- WINDOWS: ☑

**TCP PING:** ☑

**ICMP PING:** ☑

**TCP PORT:** ☑

**UDP PORT:** ☑

**SNMP:** ☑

---

**FIG. 8**
1102

PROVIDE USER SELECTED AND/OR COMPUTER SELECTED SECURITY DOCUMENTS

1104

MODIFY TESTING REQUIREMENTS?

YES

1106

DISPLAY SELECTED TEST PROCEDURE FOR MODIFICATION

1108

MODIFY TEST PROCEDURE AND SAVE

1110

MODIFY ANOTHER?

NO

END

YES

FIG. 11
<table>
<thead>
<tr>
<th>Regulation</th>
<th>Paragraph</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>BS ISO/IEC 17799:2000</td>
<td>9.2.1</td>
<td>USER ACCESS MANAGEMENT - USER REGISTRATION</td>
</tr>
<tr>
<td>BS ISO/IEC 17799:2000</td>
<td>9.2.2</td>
<td>USER ACCESS MANAGEMENT - PRIVILEGE MANAGEMENT</td>
</tr>
<tr>
<td>BS ISO/IEC 17799:2000</td>
<td>9.2.3</td>
<td>USER ACCESS MANAGEMENT - USER PASSWORD MANAGEMENT</td>
</tr>
<tr>
<td>BS ISO/IEC 17799:2000</td>
<td>9.2.4</td>
<td>USER ACCESS MANAGEMENT - REVIEW OF USER ACCESS RIGHTS</td>
</tr>
<tr>
<td>BS ISO/IEC 17799:2000</td>
<td>9.3.1</td>
<td>USER RESPONSIBILITIES - PASSWORD USE</td>
</tr>
<tr>
<td>BS ISO/IEC 17799:2000</td>
<td>9.3.2</td>
<td>USER RESPONSIBILITIES - UNATTENDED USER EQUIPMENT</td>
</tr>
<tr>
<td>BS ISO/IEC 17799:2000</td>
<td>9.4.1</td>
<td>NETWORK ACCESS CONTROL - POLICY ON USE OF NETWORK SERVICES</td>
</tr>
<tr>
<td>BS ISO/IEC 17799:2000</td>
<td>9.4.2</td>
<td>NETWORK ACCESS CONTROL - ENFORCED PATH</td>
</tr>
<tr>
<td>BS ISO/IEC 17799:2000</td>
<td>9.4.3</td>
<td>NETWORK ACCESS CONTROL - USER AUTHENTICATION FOR EXTERNAL CONNECTIONS</td>
</tr>
<tr>
<td>BS ISO/IEC 17799:2000</td>
<td>9.4.4</td>
<td>NETWORK ACCESS CONTROL - NODE AUTHENTICATION</td>
</tr>
<tr>
<td>BS ISO/IEC 17799:2000</td>
<td>9.4.5</td>
<td>NETWORK ACCESS CONTROL - REMOTE DIAGNOSTIC PORT PROTECTION</td>
</tr>
<tr>
<td>BS ISO/IEC 17799:2000</td>
<td>9.4.6</td>
<td>NETWORK ACCESS CONTROL - SEGREGATION IN NETWORKS</td>
</tr>
</tbody>
</table>
**FIG. 13**

<table>
<thead>
<tr>
<th>QUESTION</th>
<th>YES</th>
<th>NO</th>
</tr>
</thead>
<tbody>
<tr>
<td>DO FOREIGN NATIONALS HAVE ACCESS TO THE SYSTEM/NETWORK?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DOES THE NETWORK INCLUDE REMOTE TERMINALS?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DOES THE SYSTEM PROCESS INFORMATION THAT FALLS INTO TWO OR MORE SECURITY CLASSIFICATIONS?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DOES THE SYSTEM SECURITY ASSESSMENT FALL UNDER THE PURVIEW OF A 'GENERIC' OR 'TYPE' ACCREDITATION?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DOES THE SYSTEM SECURITY ASSESSMENT FALL UNDER THE PURVIEW OF A 'OPERATIONAL' OR 'SITE' ACCREDITATION?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DOES THE SYSTEM/NETWORK CONTAIN ANY WEB SITES?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DOES THE SYSTEM/NETWORK CONTAIN DATABASE(S)?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DOES THE SYSTEM/NETWORK HAVE INTERNET ACCESS?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DOES THE SYSTEM/NETWORK INCLUDE A PROTECTED DISTRIBUTION SYSTEM (PDS)?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DOES THE SYSTEM/NETWORK INCLUDE ANY PORTABLE COMPUTING DEVICES SUCH AS LAPTOPS OR PDAs?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DOES THE SYSTEM/NETWORK INCLUDE ANY WIRELESS TECHNOLOGY?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DOES THE SYSTEM/NETWORK INCLUDE HARDWARE OR SOFTWARE THAT IS NOT OWNED BY THE ORGANIZATION (E.G. EMPLOYEE OWNED OR OTHER ORGANIZATIONS)?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DOES THE SYSTEM/NETWORK INCLUDE MODEMS?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
EDIT TEST PROCEDURE '7361'

**NAME**: [7361]

**MINIMUM CAL LEVEL**: 2

**TEST LEVEL**: SETUP:
- ADMIN ACCOUNT
- LOGIN LOCALLY AS ADMIN.

**EXPECTED RESULT**: THE PLATFORM HAS THE ABILITY CONTROL ACCESS TO ALL NETWORK RESOURCES (SHARED DRIVES, PRINTERS)

**MATCHING EQUIPMENT**: ANY
- OTHER
- NETWORK DEVICES
- COMPUTER

**MATCHING OPERATING SYSTEM**: ANY
- UNIX
- WINDOWS
- DOS-VSE
- VM
- OS90
- MVS

**MATCHING SOFTWARE**: ANY
- WEB SERVICES
- OFFICE AUTOMATION
- DBMS
- REPORTING
- SECURITY
- ERP
- ENTERPRISE MANAGEMENT
- NETWORK
- NETWORK OS
- EMAIL
- GRAPHICS
- MISCELLANEOUS

**INTERVIEW**
- OBSERVATION
- DOCUMENTATION
- TESTING

FIG. 14
START

ADD/EDIT TEST PLAN INFORMATION

ASSOCIATE REQUIREMENTS TO TEST PROCEDURES

AUTOMATICALLY GENERATE, MANUALLY ADD AND/OR EDIT TEST PROCEDURES

ENTER TEST RESULTS

PUBLISH TEST RESULTS

ADDITIONAL TEST ACTIVITY?

YES

NO

FINISH

FIG. 15
2006 Ter* **ACCREDITATION**

**DEFINITION**
SYNONYMOUS WITH THE TERM AUTHORIZE PROCESSING. ACCREDITATION IS THE AUTHORIZATION AND APPROVAL GRANTED TO A MAJOR APPLICATION OR GENERAL SUPPORT SYSTEM TO PROCESS IN AN OPERATIONAL ENVIRONMENT. IT IS MADE ON THE BASIS OF A CERTIFICATION BY DESIGNATED TECHNICAL PERSONNEL THAT THE SYSTEM MEETS PRE-SPECIFIED TECHNICAL REQUIREMENTS FOR ACHIEVING ADEQUATE SYSTEM SECURITY. SEE ALSO AUTHORIZE PROCESSING, CERTIFICATION AND DESIGNATED APPROVING AUTHORITY.

**ADMINISTRATOR**
A PRIVILEGED OPERATOR WHO HAS FULL CONTROL OF ALL THE ASSETS OF THE SYSTEM. ADMINISTRATORS ARE

**RECORDS:** 100 OUT OF 109

**FIG. 20**
FIG. 22

2202

2204

2206

2208

GENERATE THREAT STRING OF REQUIREMENT CATEGORY

GENERATE THREAT STRING OF PROJECT

DETERMINE RISK OF EACH REQUIREMENT CATEGORY

DETERMINE SYSTEM RISK BASED UPON MAXIMUM RISK OF EACH REQUIREMENT CATEGORY
<table>
<thead>
<tr>
<th>GROUP</th>
<th>SUB-CATEGORY</th>
<th>SUB-SUB-CATEGORY</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 NATURAL DISASTER</td>
<td>FIRE</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>FLOOD</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>EARTHQUAKE</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>VOLCANO</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>TORNADO</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>LIGHTNING</td>
<td></td>
</tr>
<tr>
<td>7 SYSTEM FAILURE</td>
<td>HARDWARE</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>POWER</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>COMMUNICATION LINK</td>
<td></td>
</tr>
<tr>
<td>10 ENVIRONMENTAL FAILURE</td>
<td>TEMPERATURE</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>POWER</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>HUMIDITY</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>SAND/DUST</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>SHOCK/VIBRATION</td>
<td></td>
</tr>
<tr>
<td>15 HUMAN UNINTENTIONAL</td>
<td>SOFTWARE DESIGN ERROR</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>SYSTEM DESIGN ERROR</td>
<td></td>
</tr>
<tr>
<td>17 OPERATOR ERROR</td>
<td>SYSTEM ADMINISTRATOR</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>REGULAR USER</td>
<td></td>
</tr>
<tr>
<td>19 MAINTENANCE PERSONNEL</td>
<td>SYSTEM ADMINISTRATORS</td>
<td></td>
</tr>
<tr>
<td>20 HUMAN INTENTIONAL</td>
<td>AUTHORIZED PERSONNEL</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>MAINTENANCE PERSONNEL</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>REGULAR USERS</td>
<td></td>
</tr>
<tr>
<td>23 UNAUTHORIZED USERS</td>
<td>TERRORISTS</td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>HACKERS</td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>SABOTEURS</td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>THIEVES</td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>VANDALS</td>
<td></td>
</tr>
<tr>
<td>28 PHYSICAL COMBAT</td>
<td>ELECTRONIC WARFARE</td>
<td></td>
</tr>
</tbody>
</table>

FIG. 23
EDIT BUCKET 'ANTIVIRUS PROTECTION'  ? HELP

SAVE  ☑  CANCEL

NAME*: ANTIVIRUS PROTECTION

DESCRIPTION: A UTILITY THAT SEARCHES A HARD DISK FOR VIRUSES AND REMOVES ANY THAT ARE FOUND. MOST ANTIVIRUS PROGRAMS INCLUDE AN AUTO-UPDATE FEATURE THAT ENABLES THE PROGRAM TO DOWNLOAD PROFILES OF NEW VIRUSES SO THAT IT CAN CHECK FOR THE NEW VIRUSES AS SOON AS THEY ARE DISCOVERED.

GROUP*: COMPUTER SOFTWARE SECURITY

SUBGROUP*: ANTIVIRUS

WEIGHT*: MEDIUM

<table>
<thead>
<tr>
<th>NAME</th>
<th>THREAT GROUP</th>
<th>WEIGHT</th>
</tr>
</thead>
<tbody>
<tr>
<td>HUMIDITY</td>
<td>ENVIRONMENT FAILURE</td>
<td>NEGLIGIBLE</td>
</tr>
<tr>
<td>POWER</td>
<td>ENVIRONMENT FAILURE</td>
<td>NEGLIGIBLE</td>
</tr>
<tr>
<td>SAND/DUST</td>
<td>ENVIRONMENT FAILURE</td>
<td>NEGLIGIBLE</td>
</tr>
<tr>
<td>TEMPERATURE</td>
<td>ENVIRONMENT FAILURE</td>
<td>NEGLIGIBLE</td>
</tr>
<tr>
<td>VIBRATION/SHOCK</td>
<td>ENVIRONMENT FAILURE</td>
<td>NEGLIGIBLE</td>
</tr>
<tr>
<td>ADMINISTRATIVE USER</td>
<td>HUMAN INTENTIONAL AUTHORIZED</td>
<td>HIGH</td>
</tr>
<tr>
<td>MAINTENANCE USER</td>
<td>HUMAN INTENTIONAL AUTHORIZED</td>
<td>HIGH</td>
</tr>
<tr>
<td>USER</td>
<td>HUMAN INTENTIONAL AUTHORIZED</td>
<td>HIGH</td>
</tr>
<tr>
<td>ELECTRONIC WARFARE</td>
<td>HUMAN INTENTIONAL UNAUTHORIZED</td>
<td>MEDIUM</td>
</tr>
<tr>
<td>HACKER</td>
<td>HUMAN INTENTIONAL UNAUTHORIZED</td>
<td>HIGH</td>
</tr>
<tr>
<td>PHYSICAL COMBAT</td>
<td>HUMAN INTENTIONAL UNAUTHORIZED</td>
<td>MEDIUM</td>
</tr>
<tr>
<td>SABOTEUR</td>
<td>HUMAN INTENTIONAL UNAUTHORIZED</td>
<td>HIGH</td>
</tr>
</tbody>
</table>

FIG. 24
<table>
<thead>
<tr>
<th>RISK OF REQUIREMENTS CATEGORY</th>
<th>RISK OF PROJECT</th>
<th>COMPOSITE RISK</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEGLIGIBLE</td>
<td>NEGLIGIBLE</td>
<td>NEGLIGIBLE</td>
</tr>
<tr>
<td>NEGLIGIBLE</td>
<td>LOW</td>
<td>NEGLIGIBLE</td>
</tr>
<tr>
<td>NEGLIGIBLE</td>
<td>MEDIUM-LOW</td>
<td>NEGLIGIBLE</td>
</tr>
<tr>
<td>NEGLIGIBLE</td>
<td>MEDIUM</td>
<td>NEGLIGIBLE</td>
</tr>
<tr>
<td>NEGLIGIBLE</td>
<td>MEDIUM-HIGH</td>
<td>LOW</td>
</tr>
<tr>
<td>NEGLIGIBLE</td>
<td>HIGH</td>
<td>LOW</td>
</tr>
<tr>
<td>LOW</td>
<td>NEGLIGIBLE</td>
<td>NEGLIGIBLE</td>
</tr>
<tr>
<td>LOW</td>
<td>LOW</td>
<td>LOW</td>
</tr>
<tr>
<td>LOW</td>
<td>MEDIUM-LOW</td>
<td>LOW</td>
</tr>
<tr>
<td>LOW</td>
<td>MEDIUM</td>
<td>MEDIUM-LOW</td>
</tr>
<tr>
<td>LOW</td>
<td>MEDIUM-HIGH</td>
<td>MEDIUM-LOW</td>
</tr>
<tr>
<td>LOW</td>
<td>HIGH</td>
<td>MEDIUM</td>
</tr>
<tr>
<td>MEDIUM-LOW</td>
<td>NEGLIGIBLE</td>
<td>NEGLIGIBLE</td>
</tr>
<tr>
<td>MEDIUM-LOW</td>
<td>LOW</td>
<td>LOW</td>
</tr>
<tr>
<td>MEDIUM-LOW</td>
<td>MEDIUM-LOW</td>
<td>LOW</td>
</tr>
<tr>
<td>MEDIUM-LOW</td>
<td>MEDIUM</td>
<td>MEDIUM-LOW</td>
</tr>
<tr>
<td>MEDIUM-LOW</td>
<td>MEDIUM-HIGH</td>
<td>MEDIUM</td>
</tr>
<tr>
<td>MEDIUM-LOW</td>
<td>HIGH</td>
<td>MEDIUM-HIGH</td>
</tr>
<tr>
<td>MEDIUM</td>
<td>NEGLIGIBLE</td>
<td>NEGLIGIBLE</td>
</tr>
<tr>
<td>MEDIUM</td>
<td>LOW</td>
<td>LOW</td>
</tr>
<tr>
<td>MEDIUM</td>
<td>MEDIUM-LOW</td>
<td>MEDIUM-LOW</td>
</tr>
<tr>
<td>MEDIUM</td>
<td>MEDIUM</td>
<td>MEDIUM</td>
</tr>
<tr>
<td>MEDIUM</td>
<td>MEDIUM-HIGH</td>
<td>MEDIUM-HIGH</td>
</tr>
<tr>
<td>MEDIUM</td>
<td>HIGH</td>
<td>HIGH</td>
</tr>
<tr>
<td>MEDIUM-HIGH</td>
<td>NEGLIGIBLE</td>
<td>LOW</td>
</tr>
<tr>
<td>MEDIUM-HIGH</td>
<td>LOW</td>
<td>MEDIUM-LOW</td>
</tr>
<tr>
<td>MEDIUM-HIGH</td>
<td>MEDIUM-LOW</td>
<td>MEDIUM</td>
</tr>
<tr>
<td>MEDIUM-HIGH</td>
<td>MEDIUM</td>
<td>MEDIUM-HIGH</td>
</tr>
<tr>
<td>MEDIUM-HIGH</td>
<td>HIGH</td>
<td>HIGH</td>
</tr>
<tr>
<td>HIGH</td>
<td>NEGLIGIBLE</td>
<td>LOW</td>
</tr>
<tr>
<td>HIGH</td>
<td>LOW</td>
<td>MEDIUM</td>
</tr>
<tr>
<td>HIGH</td>
<td>MEDIUM-LOW</td>
<td>MEDIUM</td>
</tr>
<tr>
<td>HIGH</td>
<td>MEDIUM</td>
<td>MEDIUM-HIGH</td>
</tr>
<tr>
<td>HIGH</td>
<td>MEDIUM-HIGH</td>
<td>HIGH</td>
</tr>
</tbody>
</table>

**FIG. 25A**
### FIG. 25B

<table>
<thead>
<tr>
<th>RANGE</th>
<th>IMPORTANCE VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 - 20</td>
<td>1</td>
</tr>
<tr>
<td>21 - 40</td>
<td>2</td>
</tr>
<tr>
<td>41 - 60</td>
<td>3</td>
</tr>
<tr>
<td>61 - 80</td>
<td>4</td>
</tr>
<tr>
<td>81 - 100</td>
<td>5</td>
</tr>
</tbody>
</table>

### FIG. 25C

<table>
<thead>
<tr>
<th>IMPORTANCE VALUE</th>
<th>ADJUSTED RISK</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>-2</td>
</tr>
<tr>
<td>2</td>
<td>-1</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>+1</td>
</tr>
<tr>
<td>5</td>
<td>+2</td>
</tr>
</tbody>
</table>
FIG. 26

2602

ANY HIGH RISK REQUIREMENTS CATEGORIES?

YES → OVERALL SYSTEM RISK IS HIGH

NO → 2606

ANY MEDIUM-HIGH RISK REQUIREMENTS CATEGORIES?

YES → OVERALL SYSTEM RISK IS MEDIUM-HIGH

NO → 2610

ANY MEDIUM RISK REQUIREMENTS CATEGORIES?

YES → OVERALL SYSTEM RISK IS MEDIUM

NO → 2614

ANY MEDIUM-LOW RISK REQUIREMENTS CATEGORIES?

YES → OVERALL SYSTEM RISK IS MEDIUM-LOW

NO → 2618

ANY LOW RISK REQUIREMENTS CATEGORIES?

YES → OVERALL SYSTEM RISK IS LOW

NO → 2622

OVERALL SYSTEM RISK IS NEGLIGIBLE

2604

2608

2612

2616

2620
SELECT THE CATEGORIES TO INCLUDE IN THE COMPLETE REPORT, THEN CLICK THE GENERATE PDF BUTTON.

PROJECT REPORTS
PROGRESS: ~ 2704a
WORK PRODUCT HISTORIES: ~ 2712a
WORKFLOW HIERARCHY DIAGRAM: ~ 2706a
WORK PRODUCT USER ACCESS AND PRIVILEGES:
WORK PRODUCT NOTIFICATIONS: ~ 2710a
USERS: ~ 2714a
EQUIPMENT: ~ 2716a
PERSONNEL: ~ 2720a
SOFTWARE: ~ 2722a
AUDIT LOG: ~ 2724a
## XACTA Project Management

### ADD PROJECT/TEMPLATE

<p>| | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**OPEN STATUS**

**PROJECT NAME**

**SUBSCRIPTION EXPIRATION**

**ASSIGN USERS**

**PROPERTIES**

**DELETE**

- **DITSCAP CLASSIC PROJECT TEMPLATE**
  - SUBSCRIPTION EXPIRATION: 10/17/2002
  - ASSIGNED USERS: [ ]
  - PROPERTIES: [ ]
  - DELETE: [X]

- **DITSCAP WORKFLOW PROJECT TEMPLATE**
  - SUBSCRIPTION EXPIRATION: 10/17/2002
  - ASSIGNED USERS: [ ]
  - PROPERTIES: [ ]
  - DELETE: [X]
EDIT PROJECT 'DITSCAP CLASSIC PROJECT TEMPLATE'

PROJECT NAME: DITSCAP CLASSIC PROJECT TEMPLATE

DESCRIPTION:

SUBSCRIPTION KEY: 1233

STATUS:
- ACTIVE
- INACTIVE

AVAILABLE AS TEMPLATE:
- YES
- NO

FILE TO RESTORE FROM:

AVAILABLE TEMPLATES:
- TIER I
- DITSCAP CLASSIC PROJECT TEMPLATE
- DITSCAP WORKFLOW PROJECT TEMPLATE
- TIER II

FIG. 30
<table>
<thead>
<tr>
<th>ROLE NAME</th>
<th>DESCRIPTION</th>
<th>PROPERTIES</th>
<th>COPY</th>
<th>DELETE</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACCREDITATION TEAM LEAD</td>
<td>C&amp;A TEAM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ACCREDITATION TEAM MEMBER</td>
<td>C&amp;A TEAM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ADD NEW ROLE NAME</td>
<td>INFOSEC MANAGEMENT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CERTIFICATION AUTHORITY</td>
<td>APPROVING AUTHORITIES</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CERTIFICATION AUTHORITY POC</td>
<td>APPROVING AUTHORITIES</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DAA</td>
<td>APPROVING AUTHORITIES</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DAA POC</td>
<td>APPROVING AUTHORITIES</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DEPUTY ISSO</td>
<td>INFOSEC MANAGEMENT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISSO</td>
<td>INFOSEC MANAGEMENT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LEAD TESTER</td>
<td>C&amp;A TEAM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ORGANIZATION RESPONSIBLE</td>
<td>SYSTEM OWNER</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PROGRAM MANAGER</td>
<td>SYSTEM OWNER</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TEST</td>
<td>APPROVING AUTHORITIES</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>USER REPRESENTATIVE</td>
<td>SYSTEM OWNER</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Role</td>
<td>Organization</td>
<td>Office</td>
<td>Properties</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------</td>
<td>--------------------------------</td>
<td>----------</td>
<td>------------</td>
</tr>
<tr>
<td>EDWARDS, E JAMES</td>
<td>ACCREDITATION TEAM MEMBER</td>
<td>TIER II SUPPORT</td>
<td>MSW</td>
<td></td>
</tr>
</tbody>
</table>

**FIG. 35**
FIG. 41D