This White Paper describes the architecture developed by Formark to deliver a collaborative certification and accreditation solution to the National Nuclear Security Administration (NNSA) of the US Department of Energy. The White Paper was written in 2003 after the initial implementation but prior to its successful certification by the NNSA.

The solution, the Integrated Certification and Accreditation System (iCAS), has dramatically reduced the cost, time and effort for the NNSA to certify and re-certify that their IT systems are compliant to security requirements outlined in government policy, regulations and standards. It has also ensured that this compliance can be successfully audited.

Formark has used this architecture and technology to automate other government business processes in Canada and the US. It is currently extending the collaborative certification and accreditation architecture to incorporate the Harmonized Threat and Risk Assessment (HTRA) methodology used within the Government of Canada.

Formark, April 2010

White Paper

An Architecture for Collaborative Certification & Accreditation

An Architecture for Collaborative Certification and Accreditation

Much of the content in this white paper is based on the participation of Ranier Systems Inc., Formark® Ltd., NCI Information Systems, Inc. and Open Text Corporation in the definition, design, development and deployment of the Integrated Certification & Accreditation System (iCAS) under a contract with the National Nuclear Security Administration (NNSA).

A major concern for both private and public sector organizations is ensuring the security of IT systems, networks and applications. As computer systems have become an essential ingredient of financial transactions, the delivery of healthcare and control systems for everything from airlines to water treatment to nuclear power facilities, even a single security breach by terrorists or white-collar criminals could have devastating consequences in terms of financial loss, violations of privacy or even the risk of injury or death. But just having authentication, encryption and other security tools is not enough – organizations also need a clear, proven methodology to ensure the tools are being applied properly.

Just as the international manufacturing community created the ISO 9000 standards defining a methodology for ensuring quality in manufacturing environments, governments around the world have collaborated to create international standards that define methodologies for verifying the security of computer systems. Systematically applying these standards and other national standards to a computer system about to be deployed (known in security parlance as “certification and accreditation” or “C&A” for short) is a non-trivial task, especially for systems with many components. The challenges involve collecting compound sets of configuration data; managing large numbers of test descriptions; tracking hundreds of task workflows and assembling complex electronic documents.

A collaboration and knowledge management platform, such as Livelink® from Open Text Corporation, provides an excellent starting point for building an architecture for automating the certification and accreditation process. By leveraging Livelink's underlying document management and workflow capabilities, a Collaborative C&A application can dramatically reduce the time and cost of the certification process by guiding the security personnel through the required steps and automatically handling all of the process bookkeeping along the way.

Security Assurance for IT Systems

The never-ending quest to build more secure IT systems demands the effective coordination and continual improvement of the key ingredients:

- Well defined system-level security requirements and security specifications
- Well designed component products
- Sound systems security engineering practices
- Competent systems security engineers
- Appropriate metrics for product/system testing, evaluation, and assessment
- Comprehensive system security planning and life cycle management

More secure IT systems cannot be created in isolation in an artificial laboratory environment – it requires a comprehensive approach that links the critical assessment activities both in a testing environment and in the real-world environment where the system will be operating.

A crucial element of this comprehensive approach is Certification & Accreditation. The first step, certification, is a standard, proven methodology that ensures all applicable tests are systematically performed against each system and its components, in their intended operating environment. The test results are evaluated and if required, steps are taken to correct or to mitigate the impact of any failed tests. The output of the validation phase is a very complete report describing the IT system, its operating environment, the security requirements, the tests performed, the results of the tests and an assessment by qualified security professionals of the risks and vulnerabilities of the system. This report is presented to the agency that will be re-

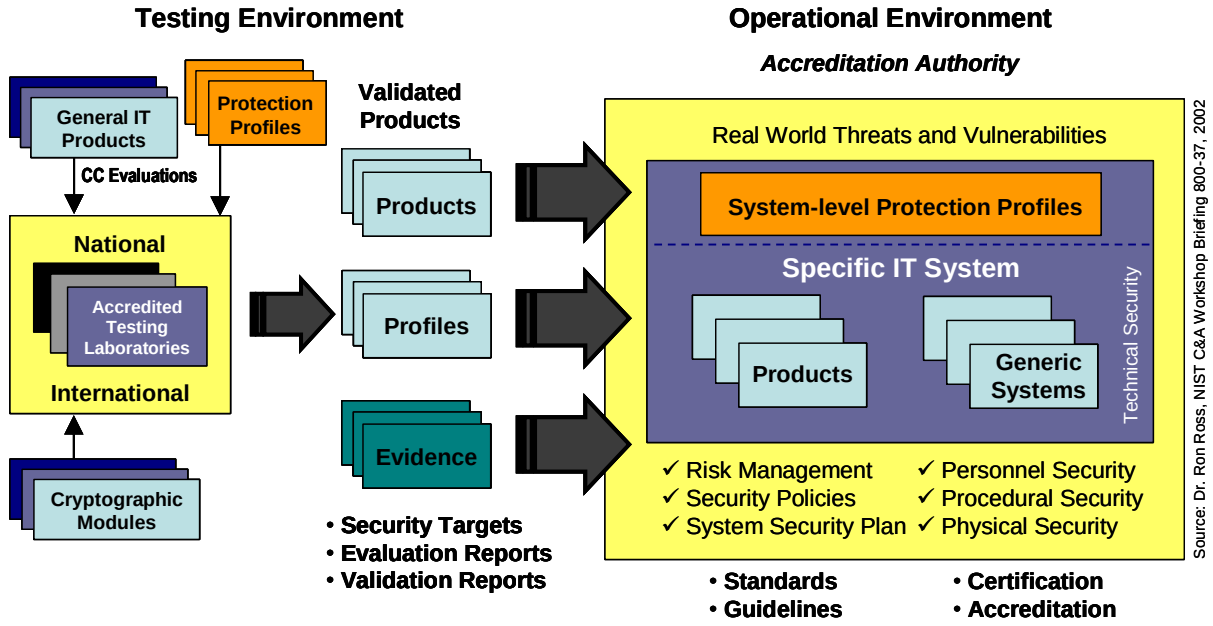


Figure 1 Secure assurance requires a comprehensive approach that verifies tested products in the working operational environment where they will be used.

sponsible for accepting the risk and approving the operation of the system.

Accreditation is a management decision by a senior official in the organization, to authorize the operation of the IT system based on the results of the certification and other relevant considerations. Certification and Accreditation is not about risk avoidance, but rather it is about risk management. By granting accreditation, the senior official, often referred to as the Designated Approving Authority (DAA), accepts responsibility for the safe and secure operation of the IT system. In doing so, the DAA must balance the mission requirements of the organization (and hence the need to operate the IT system) and the residual risks to the IT system after applying the appropriate protection measures, typically in the form of security controls.

Standards

International standards for security and security methodologies provide a generic framework which each country or industry group can augment with their own specific requirements to create their own certification and accreditation standards. For example, many agencies in the US Government are legislatively required to combine standards defined by the National Institute of Science and Technology (NIST) and the National Information Assurance Partnership (NIAP), such as FIPS 140-2 and National Information Assurance Certification and Accreditation Process (NIACAP), along with the international ISO/IEC 15408 Common Criteria methodology (see www.commoncriteria.org). Other agencies will have a different selection of standards that must be applied.

One key standard, the ISO/IEC 15408 Common Criteria methodology, was developed by combining work done by the United States, Canada, United Kingdom, France, Germany and the Netherlands, and the ongoing collaborative effort to create consistent and useful security methodologies is now supported by numerous other countries throughout the world.

To have broad applicability, these standards must be defined in generic terms. To apply the standards, governing bodies typically will interpret the standards into more specific terms and will collect related elements from multiple standards into a set of directives referred to as protection profiles. It is these profiles which are then applied to a given IT system in the certification and accreditation process.

Collaborative Certification and Accreditation

Systematically applying these protection profiles to an IT system can be a very non-trivial task, especially for network-based IT systems with many components. There can be hundreds or thousands of configuration parameters, which intersect with multiple protection profiles to produce hundreds of individual tests that must be documented, approved, performed, recorded and analyzed. Plans must be published, approvals must be tracked, audit information recorded, and everything must be saved for archive and subsequent re-use as systems and operating environments undergo changes.

At the current time, the technology available to assist in this process primarily consists of single-purpose tools that address only one part of the overall process. What is required is an end-to-end certification and accreditation application that not only integrates the electronic ingredients – the configuration data, security requirements, test descriptions, etc. – but also integrates the people into the process through workflow and collaboration.

Elements of an Architecture

To create an integrated C&A application, the following key capabilities are required:

1. **Collaboration and Document Management**. All of the participants in the C&A process must be able to share information with each other. A collaboration and knowledge management platform, such as Livelink from Open Text Corporation, provides an excellent framework for connecting people to each other and to automated processes.
2. **Configuration and Requirements Database**. The system must be able to capture the information about the IT system and its operating environment that is needed to verify that it meets the security requirements. To automate the interaction between the system configuration and the security requirements, the requirements must be defined electronically in a way that describes exactly how they relate to the configuration.
3. **Workflow**. Certification and accreditation is a process which has an implicit set of steps or workflow to be followed. Inside each major step in the process can be hundreds of independent tasks that can each have their own workflow. Automating the tracking of the work is essential to dealing with the complexity of large systems and environments.
4. **Role-based User Interfaces**. The ideal user interface should be Web-based to allow access over a network, using pages that are designed specifically for the task being performed and the user doing the work, whether they are managers, security officers or testers. The objective must be to keep the users focused on the task at hand without being distracted or overwhelmed by numerous options that aren't relevant at the moment. This facilitates the distribution of tasks among all of the parties that can participate in the certification and accreditation process.
5. **Automation**. Currently many of the steps in the certification processes are tedious, repetitive and prone to errors when done manually. Numerous tasks can be automatically performed by independent agents (*i.e.* no user interface) or tailored logic behind the role-based user interfaces that are designed to solicit input and decisions from the users. It is the supporting automation behind them that allows the role-based user interfaces to be simple and easy to use.
6. **Document Assembly**. A specialized form of automation is document generation and assembly. The certification process requires the generation and management of hundreds of independent snippets of information (*e.g.* a test description), which are best maintained in a natural source format that allows maximum flexibility and editing. Only when a document is actually required should the content be assembled from the different sources and formatted as a document. This approach also ensures that all subsequent documents will have the latest version whenever a common section of content is revised.

By combining all of these capabilities to create an integrated application, it is estimated that certification and accreditation projects using such an application can eliminate up to 90% of the time currently required to execute the processes manually.

Operational Benefits

The return on investment (ROI) for a collaborative C&A application will be evident both in the short term and over the long term. Immediate operational and cost containment benefits include:

1. Dramatically shorter time to certify an IT system, which enables systems to be deployed sooner and allows more certifications to be done with existing resources.
2. Automation of time-consuming manual tasks enables skilled testers to spend a greater percentage of their time on the high-value testing tasks that require their expertise.
3. Managing the testing documents in electronic form significantly reduces the costs associated with handling, storing and transporting paper documents.
4. Greater accuracy and consistency in the way certifications are done improves the confidence in the security of deployed systems and reduces the inclination to re-certify systems already certified by another facility or organization.
5. Automated workflow and task-oriented user interfaces reduce the time required to train testers and other security personnel.

Strategic Benefits

A collaborative C&A application will not only make the existing certification process dramatically more efficient, but it can also provide significant long-term strategic benefits:

1. Aligning with the “paperless office” initiatives within governments at all levels.
2. Creating a configuration database which allows organizations to readily identify which systems are affected by new security threats or updates needed to close security holes.
3. Enabling vendors to “pre-certify” systems to further reduce the lead time for system deployments.

Collaborative C&A in Action

The goal of a C&A process is to produce a security plan that documents the certification process and can be used by the organization to make an informed decision to grant accreditation to the IT system. The following section outlines a typical six-step process and highlights how a collaborative C&A application would assist organizations to perform each step.

1. Definition Phase

(a) Describe the security objectives of the certification process and choose the protection profiles, guidelines and regulations with which the secure system must comply.

(b) Define the IT system and its operating environment.

(c) Identify the individuals with the key roles in the process, such as the Designated Approval Authority and other security officers.

At installation time the application administrator organizes all of the standards and regulations that the application can handle into security profiles. The profiles can be specified as mandatory across the organization, mandatory for a given facility or optional at the discretion of the security officer who creates each new C&A project.

When the project is created, the application then requires the security officer to select which security profiles will apply, then guides the security officer through a structured set of menus in which each component of the IT system is identified, and all its parameters (based on what is needed by the security profiles) are collected and saved in a database for use in subsequent phases. Even modest systems can involve dozens of components and hundreds of individual parameters and variables.

2. Verification Phase

(a) Select the tests that must be performed to meet the security requirements.

(b) Include any local requirements and tests to verify them.

(c) Create the initial security plan.

(d) Obtain DAA review and authorization of the plan.

With the starting point (the IT system configuration) and the desired end point (the security requirements) defined, the application iterates through all of the IT system components and selects those tests that must be performed on the secure system to ensure compliance.

The generic description of each test is retrieved from the database and/or the document management system, and is customized with the IT system information gathered in the configuration step. This ensures the descriptions in the security plan are explicit and specific enough for the testers to apply the tests properly.

The application then automatically generates the security plan, describing the security objectives and all of the tests needing to be performed on the IT system in order to reach that objective. There may be many hundreds of tests, resulting in massive documents running to many hundreds of pages in size.

The security plan is submitted to the DAA who verifies the security requirements and tests, then digitally signs the document indicating that the next phase can proceed.

3. Validation Phase

(a) *Perform system component and operating environment testing.*

(b) *Record results of all tests.*

Each test indicates the skills the tester must have (e.g., administrator-level knowledge of the operating system) in order to properly perform the test. Each person defined as a potential tester also has an associated set of skills they possess. The application uses this information to distribute each test into a workflow queue that will only be accessible by testers who have the required skills.

As each tester logs into the application, they see only the tests they are qualified to perform that still need to be done. When the tester chooses a test from the list, they are presented with the customized test description. Once they have performed the test on the system being evaluated and the test results have been recorded, they return to select another test and the cycle repeats.

When the last test has been completed, the application automatically assembles an updated security plan that now includes all of the test results.

4. Risk Assessment Phase

(a) *Evalutate failed tests and document how the risk will be mitigated:*

- *Impact statement*
- *Countermeasure*
- *Risk acceptance*

(b) *Present final plan and certification recommendation for approvals.*

The application enables some failed tests to be redone if they failed due to errors in the configuration, or some other correctable situation. Otherwise the security officer is required to provide written assessment of the impact, other countermeasures and risk acceptance.

Once all the mitigation steps have been taken, the application requires the security officer to make a recommendation as to whether the system can be deployed and operated. These risk assessments and the certification recommendations are assembled into the final version of the security plan, which is digitally signed by the security officer(s).

5. Publishing Phase

(a) *Security officers review and sign off on the security plan*

(b) *Present DAA with certification recommendation, and accreditation options (approval, interim approval, rejection).*

(c) *After DAA determines the disposition, the complete plan is to be published*

The application moves the final security plan through the workflow needed to gather all required digital signatures, and automatically generates the appropriate recommendations and accreditation options based on the choices by the security officer(s).

In the final step of this workflow, the application routes the plan, along with the certification recommendation, to the DAA and presents the accreditation choices. Once the DAA makes a determination and digitally signs off on it, the application seals and publishes the final version of the plan, and sends a notification of the decision to the security manager and the system owner.

6. Post-Accreditation Phase

(a) *Maintain the security plan*

(b) *Update based on changes to hardware, software, security requirements or policy*

The application allows security officers to apply changes to a copy of the original configuration. This enables them to quickly evaluate the potential impact of changes in order to determine if a full re-certification is required.

Maintaining the security plan significantly reduces the time and cost to re-certify systems.

Features and Benefits

An effective collaborative certification and accreditation application will also provide many immediate and pragmatic benefits throughout and following the C&A process, as shown in the table below.

Table 1 Features and Benefits of a collaborative certification and accreditation architecture.

Feature	Benefit
Structured menus for entering required configuration information	Eliminates the need to manually determine which information is required for each type of component
Ability to define organizational or facility-specific security profiles	Ensures consistent application of security policies and standards across many systems and many facilities throughout an organization
Automatic cross-reference of IT system configuration against security requirements	Dramatically less time required to generate the list of tests that must be performed. Eliminates errors
Automatic customization of test descriptions with configuration information	Dramatically less time required. Ensures testers have explicit instructions, leading to fewer errors
Automatic assembly of security plan document	Dramatically less time required and ensures completeness and correct versions
Direct source-to-PDF document assembly	Eliminates conversions to/from intermediate file formats and gives full control over the format of published documents
Requirement for electronic signatures on generated PDF documents	Ensures no changes are deliberately or inadvertently made to the test plan, and establishes a complete audit trail
Automatic distribution of tests to qualified security testers	Much less time required to cross-reference tests against tester skill sets
Testers provide test results on the same screen as the test description	Ensures that the test results are correctly associated with the test
Automatic assembly of test results document	Dramatically less time required and ensures completeness
Managers can immediately see the state of the certification process	Managers have “early warning” of bottlenecks or capacity problems and can take corrective action sooner
All activities are logged	Complete audit trail
Ongoing retention of the configuration database	Eliminates need to completely start over again when policy requires that systems be re-certified every few years or whenever some component in the system changes. The application will retain all of the documents and the configuration databases to provide a ready starting point for any follow-on re-certification projects

Case Study – National Nuclear Security Administration

The US Government – National Nuclear Security Administration (NNSA) – has years of real world experience in the deployment of large-scale IT systems. As part of NNSA's ongoing commitment to using a comprehensive approach to security assurance, the administration initiated the NNSA Integrated Certification and Accreditation System (iCAS) project to systematically automate the Information System Certification and Accreditation Process (ISCAP).

iCAS also incorporates best practices from national and international Certification and Accreditation standards – it specifically implements the (NIST 1000) National Information Assurance Certification and Accreditation Process (NIACAP) 5-step process and incorporates the ISO/IEC 15408 Common Criteria methodology to perform backend security requirements processing.

iCAS Functionality

The objective of iCAS is to automate the certification and accreditation process. The current C&A process can include manually assembling a security plan that can total more than 800 pages of information for a complex IT system – a feat that can take months to complete. Once the testing is completed, the final System Security Plan document may be more than 1,500 pages long. Clearly this level of effort and the elapsed time needed to complete the process has a major impact on the ability of the NNSA to deploy needed systems. The requirement to have IT systems re-certified every three years and whenever there are significant hardware or software changes, only magnifies the overall cost to the organization.

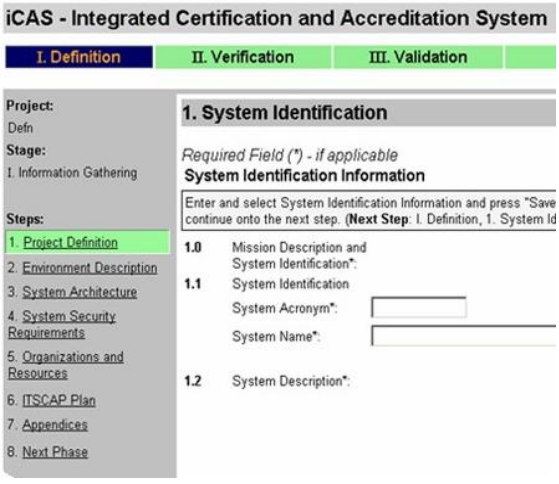


Figure 2 Role-base user interface

iCAS Project Status

- The initial requirements analysis and product selection was done by NCI Information Systems under contract with NNSA.
- The design phase of the project selected Livelink from Open Text as the underlying collaboration and document management platform, and chose the Formark Outside development environment for building the application on the Livelink platform.
- The development of the iCAS application was done by Ranier Systems and Formark, under a contract with NNSA.
- NCI Information Systems is providing maintenance and operations services for iCAS.
- The iCAS solution is a Government Off-The-Shelf (GOTS) product developed using Commercial Off-The-Shelf (COTS) software.
- iCAS is owned by the NNSA.
- As of April 2003, the initial implementation of iCAS is currently under review by NNSA Cyber Security Office for NNSA policy compliance.

Virtually all of the individual steps in the C&A process are relatively straightforward – the complexity arises in the inter-relationships and the massive number of combinations and permutations that can exist among the security requirements, the hardware and software configurations, the tests to be performed and the tester skill sets. iCAS protects the users from the complexity by providing a gated workflow that leads the security officers through each step of the process – information gathering, generation of the System Secu-

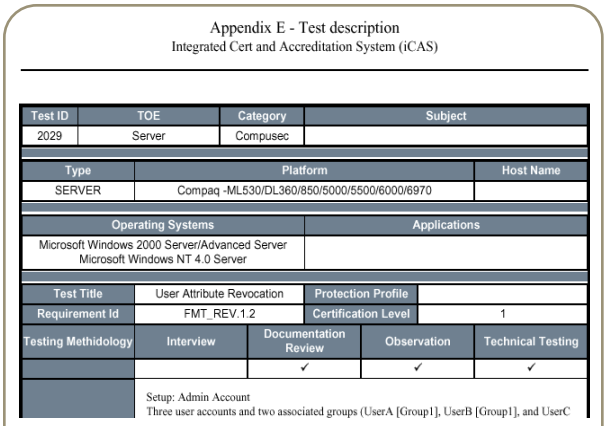
rity Plan, tracking the test results and the creation of the final version of the System Security Plan.

iCAS uses Livelink to manage the many documents, test descriptions and templates, along with a database containing the security requirements, the configuration data and the test results.

iCAS relies exclusively on a role-based user interface, similar to the one in Figure 2, that are tailored to each user's role in the process and the task at hand. The iCAS interface presents a spreadsheet-like screen, with the major stages across the top, the required steps down the left side, and the details of the current step in the middle. This design makes it easy for users to be guided from one step to the next while still enabling expert users to jump directly to a desired place in the process. iCAS controls the major workflow stages along the top and will not allow users to move to the next stage until the current stage has been completed.

iCAS uses automation to do most of the routine activities in the process. Once the configuration data is collected, an automatic agent is launched to determine all of the tests that must be performed in order to comply with the protection profiles chosen by the security officer. After selecting all the tests to be done, iCAS produces a description of each test (encoded in XML) that is customized with the configuration information to ensure the test descriptions are specific enough to be understood and executed properly by the testers.

iCAS then assembles (directly from XML-framed text fragments into a PDF document) all of the collected and generated information into a System Security Plan to be reviewed and digitally signed by the appropriate security officer.



Appendix E - Test description
Integrated Cert and Accreditation System (iCAS)

Test ID	TOE	Category	Subject
2029	Server	Compusec	

Type	Platform	Host Name
SERVER	Compaq -ML530/DL360/850/5000/5500/6000/6970	

Operating Systems	Applications
Microsoft Windows 2000 Server/Advanced Server Microsoft Windows NT 4.0 Server	

Test Title	User Attribute Revocation	Protection Profile	
Requirement Id	FMT_REV.1.2	Certification Level	1

Testing Methidology	Interview	Documentation Review	Observation	Technical Testing
		✓	✓	✓
	Setup: Admin Account Three user accounts and two associated groups (UserA [Group1], UserB [Group1], and UserC			

Figure 3 iCAS Test description

Once approved, iCAS moves to the validation stage where the first task is to automatically assign each of the potentially hundreds of testing actions to the workflow queues of testers who are qualified to perform the test. As each tester logs into iCAS they are presented with a list of only those tests that they are qualified to perform on the system being evaluated. Once the last test is completed, another automated agent assembles all of the test results into yet another massive document for review of the risk assessment by the security officers.

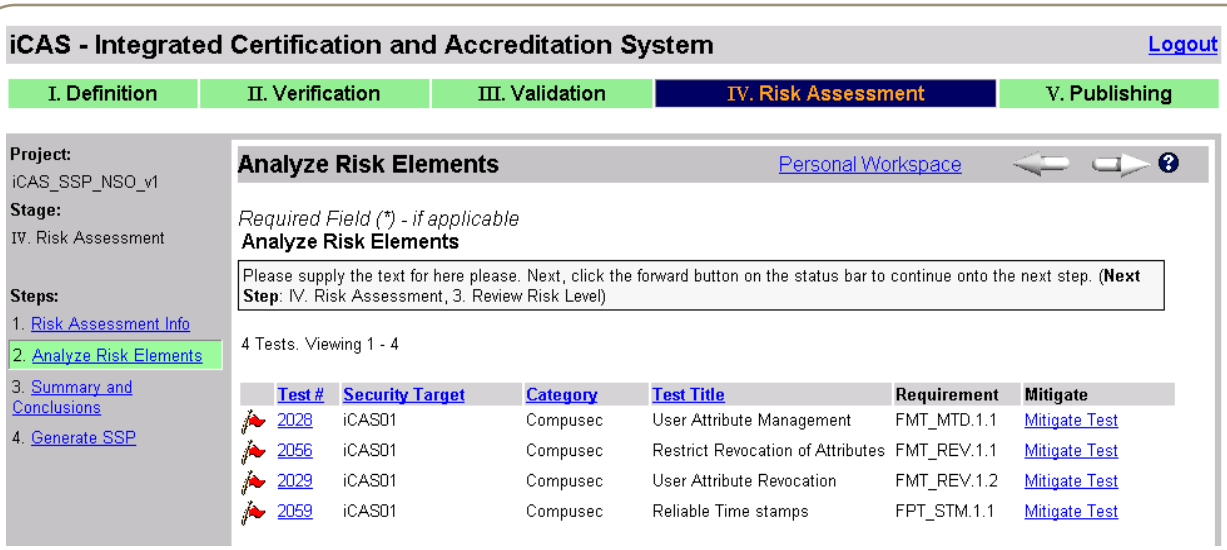


Figure 4 Risk Assessment Phase allows security officer to specify risk mitigation information

As per the C&A process, once all of the risk assessments are completed, a final System Security Plan is produced for the Designated Approval Authority (a senior manager within NNSA) to review and decide whether or not to grant accreditation to the secure IT system.

iCAS ROI

Although still at the early stages of deployment, indications are that the productivity improvements and associated cost savings are staggering. Process stages which may currently take six months to complete can now be completed in one tenth of that time. The time and cost savings may be even higher down the road when the secure IT systems need to be re-certified and the security officers can start the process with all of the configuration data already in place. A major strategic benefit is that over time the database will contain the configuration data for all the systems within a facility or across the entire NNSA, which will allow security officers to instantly determine which secure systems are affected by the rise of a new threat or the discovery of a new vulnerability and respond accordingly.

iCAS is continuing to be developed and expanded.

Summary

As the NNSA experience with iCAS shows, solutions built using a Collaborative Certification and Accreditation architecture will offer clear and quantifiable benefits for organizations that must certify the security of deployed IT systems.

About Formark

Formark is a leader in helping organizations to reduce costs, time and effort, and increase effectiveness through the automation of private and public sector business processes.

An Open Text Affinity Partner since 1996, Formark became a Certified Microsoft Solution Partner in 2007.

For more information visit our website at **www.formark.com** or contact Formark at **(613) 599-5173 x230** or **sales@formark.com**.

50 Hines Road, Suite 150
Kanata, Ontario K2K 2M5
t. 613.599.5173 *f.* 613.599.6217

For more information, please visit:
www.formark.com