White Paper: Risk Management and Compliance with NIST SP 800

Imprimis, Inc.
5755 Mark Dabling Blvd.
Suite 250
Colorado Springs, CO 80919
June 2016

This white paper describes the requirements for a sound cybersecurity program, the need and proper use of standards, a description of the NIST SP 800 Series Cybersecurity Standards, the requirements imposed by recent DFARS and FAR clauses, options available, presents the Imprimis, Inc. Assessment and Compliance Tool (i2ACT-800), describes the capabilities of the tool and discusses the many advantages of using the i2ACT-800.

TABLE OF CONTENTS

TABLE OF FIGURES

INTRODUCTION

Cybersecurity is a broad reaching term that is not well understood today. The threats posed by the lack of cybersecurity present an unprecedented threat to the United States and the free world. Cyber-attacks threaten our current way of life, competitiveness in the global market, and have the real capability to damage and destroy. Destruction occurs in critical infrastructure such as the electric grid, pipelines, healthcare, finance and many more. Destruction also comes in the form of cybercrime which is the theft of both money and intellectual property. Espionage, disruption of service, sabotage, and terrorism round out the cyber threat portfolio.

Much of future innovation will first be born in the cyber domain before it enters the physical domain. Health related systems and technology, the factory of the future, and the smart grid are examples of 'cyber first' future businesses. These and future enabling cyber-based technologies will be created and realized in a cyber domain that is both free and secure.

The need for cybersecurity is of paramount importance and must be applied widely and consistently. A chain is only as strong as its weakest link. This is absolutely true of cybersecurity. To date, most cybersecurity resides in the government or major organizations with the knowhow and resources required. Small businesses, if not secured in the cyber space, can and will be the weak link and will facilitate 'vectoring' which is allowing the attackers to unwittingly use them to reach larger and more secure targets. The cyber-attack on Target is a perfect example. This giant retailer was successfully compromised by a cyber-attack that was facilitated by a HVAC contractor.

Cybersecurity is not a technology challenge alone. The three major components involved in successful cybersecurity defense include Policy, Behavior, and Technology (FIGURE 1). Policies are defined by the leadership of an organization and define the structure for successful cybersecurity at an organizational level.

Most sources say more than 80% of breaches occur through the accounts of people authorized to use the network. Phishing emails, spear phishing e-mails, and whaling cause most of the damage when an employee or authorized person opens an email or follows a link that leads to an infection. Poor password controls and other access breaches do the rest.

Technology is making great strides in strengthening the perimeter defenses (firewall, IDS/IPS, 2FA, etc.) and active monitoring is raising the security bar. However, the people using the system must do their part for cybersecurity and the capability of cybersecurity technology must grow to meet future challenges. People and technology must work together to ensure cybersecurity.

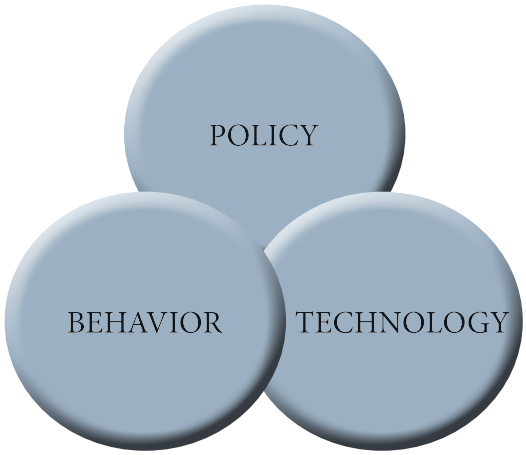

FIGURE 1: Components of Cybersecurity Defense

WHY CYBERSECURITY STANDARDS?

Lewis Carroll's Cheshire Cat in Alice in Wonderland turned the phrase "If you don't know where you are going, any road will get you there." It logically follows that if you do not know where you are going, you will not know if and when you have arrived!

> "If you don't know where you are going, any road will get you there".
> … and you will not know when you have arrived! Lewis Carroll

The purpose of standards is to help you determine where you need to go and help measure your progress in getting there. They represent the accumulated knowledge, experience, and wisdom of many who have traveled the road before you. Standards (FIGURE 2) are documents produced after great collaborative efforts of experts and are meant to establish normal requirements, guidelines or practices for an item, system, or process to ensure the appropriate outcome in terms of performance, quality, and cost. Technical standards, i.e. cybersecurity standards, pertain to technical systems such as a complex IT network with many applications running over the network and through numerous connections to the global internet.

Standards are developed and promulgated across many users to provide consistent outcomes. They also contain the wisdom of all who contributed. Thus standards must be developed, promulgated and used to implement effective cybersecurity in organizations - large and small. Disciplined application of standards tends to provide better quality, lower costs, and enables organizations, large and small, to become far more competitive.

3.2 standard *[ISO/IEC Guide 2:1996, definition3.2]*

". . . document, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context."

NOTE – Standards should be based on the consolidated results of science, technology and experience, and aimed at the promotion of optimum community benefits.

FIGURE 2: Technical Standard Example

CYBERSECURITY STANDARDS

There are a number of standards published and in use today. The major standards used for information and network security are shown in FIGURE 3. The ISO27000 series is the predominant international standard. The NIST (National Institute for Standards and Technology) Special Publications 800 series is the standard for the U.S. Government and is being adopted by local government and private organizations. NIST was given the responsibility of establishing a risk management framework for securing government networks with the passage of the Federal Information Security Management Act of 2002 (FISMA; 44 U.S.C. §§ 3541-3549). The Special Publications, initiated by NIST in 1990, were seen as the ideal platform for building the national cybersecurity framework. The Special Publications (800 Series) is the result of extensive research and collaboration with industry, academic, and government organizations; and are applicable to the same organizations.

STANDARD	TITLE	SPONSORING ORGANIZATION
ISO 27000 Series	International Information Security Management System (ISMS)	ISO (International Organization for Standardization
ISA/IEC-62443	Industrial Network and System Security	ISA (International Society for Automation) ANSI (American National Standards Institute)
NERC Standards	Reliability Standards for the Bulk Electric Systems of North America	NERC (North American Electric Reliability Corporation) Standards Institute)
COBIT	Control Objectives for Information and Related Technology	ISACA (Information Systems Audit and Control Association) Standards Institute)
NIST SP 800	NIST Special Publications	NIST (National Institute of Standards and Technology) Standards Institute)

FIGURE 3: Types of Cybersecurity Standards

CYBERSECURITY FRAMEWORK

NIST acting under the direction of the Executive Order 13636 "Improving Critical Infrastructure Cybersecurity", February 12, 2013, has developed a framework that allow organizations at all levels to address cybersecurity needs in an organized manner. As stated in the NIST publication "Framework for Improving Critical Infrastructure Cybersecurity" (National Institute of Standards and Technology, February 12, 2014,), the Framework provides a common taxonomy and mechanism for organizations to:

1) Describe their current cybersecurity posture;
2) Describe their target state for cybersecurity;
3) Indentify and prioritize opportunities for improvement within the context of a continuous and repeatable process;
4) Assess progress toward the target state;
5) Communicate among internal and external stakeholders about cybersecurity risk.

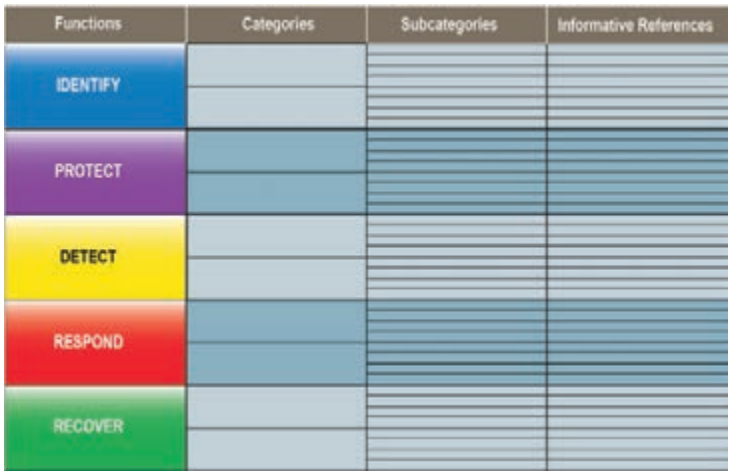

FIGURE 4:Cybersecurity Framework Core Structure

The core of the framework is shown in FIGURE 4. Properly utilized, the Framework involves personnel in all levels of the organization

from leadership through all who implement the framework. The implementation of the Cybersecurity Framework relies on standards, guidelines and practices. NIST has provided numerous publications to assist organizations and one of the main family of publications is the NIST Special Publications 800 which encompass the Risk Management Framework (RMF).

THE NIST RISK MANAGEMENT FRAMEWORK

The SP 800 series begins with SP 800-1 and has evolved to include NIST SP 800-171 "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" as well as several additional standards and guidelines out for comment in draft form. It addresses all types of computer based networks including industrial control systems. It is constructed in a manner that allows most of the standards to address procedures and considerations in specific applications while at the same time providing an exhaustive list of security controls, a subset of which can be applied in all applications. NIST clearly recognizes that one size does NOT fit all organizations. Careful consideration of threats, risks, and critical assets, combined in the standard procedure, will yield the appropriate security profile or baseline for an organization. This is referred to as the Risk Management Framework (RMF).

The RMF approach involves a tiered risk management approach including the highest levels in the organization, the mission or business processes, and the operational environment (FIGURE 5). This process is described in NIST SP 800-37. All stakeholders must be included for a successful security program. The highest level is responsible for the policy and governance of the organization and the security framework. This is the leadership of the organization and if they are not actively involved, the framework will fail. During the organizational review and requirement setting in Tier 1, risk from an organizational perspective is examined so that a comprehensive risk management strategy can be developed for the entire organization including the:

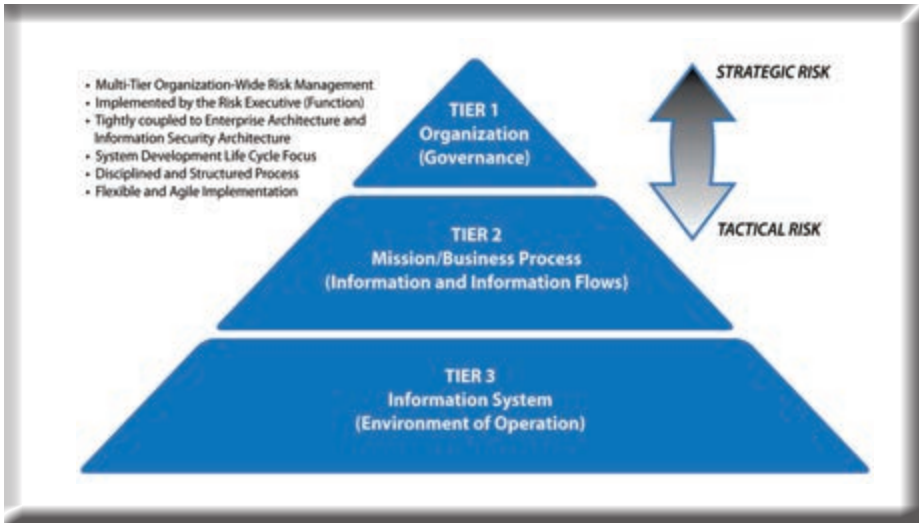

FIGURE 5: RMF for Multi-Tier Organizations

1. techniques the organization plans to employ to assess information system-related security risks;
2. procedures the organization will use to evaluate the significance of the risks identified;
3. risk mitigation measures the organization plans to use;
4. level of risk the organization will accept (i.e., risk tolerance);
5. ongoing risk monitoring the organization plans to perform; and
6. risk management oversight and continuous evaluation that will be implemented.

The risk management strategy is then propagated to key officials within the organization for implementation. The organizational officials will include:

1. authorizing officials;
2. chief information officers;
3. senior information security officers;
4. enterprise/information security architects;
5. information system owners/program managers;
6. information owners/stewards;
7. information system security officers;
8. information system security engineers;
9. information system developers and integrators;
10. system administrators;
11. contracting officers; and
12. users

The middle tier is the mission or business process tier. The key issue for this tier is to ensure the success of the organization by assuring the availabilty and effectiveness of the business operations. The security framework should be built around the processes of the organization which were designed to achieve the mission of the organization. The operational tier, or tactical tier, is the organizational infrastructure designed to support the processes of the organization and the information systems that are a

critical part of the organizational infrastructure.

The RMF involves 6 steps (FIGURE 6). The six steps include: categorizing your system in terms of potential risk, selecting the controls to be used in protecting the system, implementing the controls, assessing the compliance status of the controls, authorizing operations, and monitoring. This process is repeated periodically, or as required, to ensure compliant operations.

The starting point (step 1) calls for the categorization of the information system and this requires the identification of the threats, risks, vulnerabilities and the requirements of the mission oriented business processes. The RMF designs security around three major priorities – Confidentiality (C), Integrity (I), and Availability (A). The risk categorization includes three impact levels – Low (limited adverse effects), Moderate (moderate adverse effects), and High (severe or catastrophic adverse effects). The Risk Categorization Matrix is shown in FIGURE 7.

FIGURE 6: RMF Steps

In most cases, the baseline of controls has been defined based on the categorization and the standard applied. The Federal Information Processing Standards (FIPS) use a high water mark in that the

C-I-A	LOW IMPACT	MODERATE IMPACT	HIGH IMPACT
Confidentiality (C) **Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]**	The unauthorized ***disclosure of information*** could be expected to have a ***limited adverse effect*** on organizational operations, organizational assets, or individuals.	The unauthorized ***disclosure of information*** could be expected to have a ***serious adverse effect*** on organizational operations, organizational assets, or individuals.	The unauthorized ***disclosure of information*** could be expected to have a ***severe or catastrophic adverse effect*** on organizational operations, organizational assets, or individuals.
Integrity (I) **Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]**	The unauthorized ***modification or destruction of information*** could be expected to have a ***limited adverse effect*** on organizational operations, organizational assets, or individuals.	The unauthorized ***modification or destruction of information*** could be expected to have a ***serious adverse effect*** on organizational operations, organizational assets, or individuals.	The unauthorized ***modification or destruction of information*** could be expected to have a ***severe or catastrophic adverse effect*** on organizational operations, organizational assets, or individuals.
Availability (A) **Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]**	The ***disruption of access to or use of information*** or an information system could be expected to have a ***limited adverse effect*** on organizational operations, organizational assets, or individuals.	The ***disruption of access to or use of information*** or an information system could be expected to have a ***serious adverse effect*** on organizational operations, organizational assets, or individuals.	The ***disruption of access to or use of information*** or an information system could be expected to have a ***severe or catastrophic adverse*** effect on organizational operations, organizational assets, or individuals.

Federal Information Processing Standards Publication, FIPS PUB 199, February 2004, National Institute of Standards and Technology

FIGURE 7: Risk Categorization Matrix

highest risk category defines the baseline of security controls. The Committee of National Security Systems (CNSS) has issued Instructions (CNSSI-1253) that provide baselines for C, I, and A independently and do not use a high water mark. An individual organization can select their own baseline of security controls or modify one of the recommended baselines.

Implementation of the cybersecurity controls follows and includes remediation to ensure the system is in fact complying with all controls in the selected baseline. Once compliance has been verified, the system is authorized and then put into operation. The system should be continuously monitored, and adjustments made as indicated. The RMF process is repeated as necessary.

REQUIREMENTS: DFARS & FAR

The Defense Federal Acquisition Regulations Supplement (DFARS) added the prescriptive language in DFARS Subpart 204.73 for contracts to use the clause at 252.204-7012, titled "Safeguarding Unclassified Controlled Technical Information (UCTI)" as a requirement for all contractors doing work with the Department of Defense (DoD) in November of 2013. Little happened following the publication of the 'cyber DFARS'. Gradually, the prescribed clause was introduced into more and more contracts. Two years following their introduction, the clause was being included in almost all contracts issued from any DoD organization.

Covered Defense Information (CDI):

Unclassified information that is

i) Provided to contractor by or on behalf of DoD,
ii) Collected, developed, received, transmitted, used, or stored by the contractor, or [information that] falls within the following categories

i) Controlled technical information,
ii) Critical information (operations security),
iii) Export control,
iv) Any other information, marked or otherwise identified in the contract thatrequires safeguarding or dissemination controls

FIGURE 8: CDI Definition

The DFARS subpart and clauses were changed dramatically in August of 2015. They now call for the use of NIST (SP) 800-171, included subparts and clauses for cloud computing, and strengthened the reporting requirements. Key in all of these changes was requiring the protection of Covered Defense Information (CDI) rather than the original UCTI. The definition of CDI (FIGURE 8) includes UCTI and much more. Subpart 204.73 was renamed as was clause 252.204-7012 (FIGURE 9) and two additional clauses were prescribed under 204.73. Definitions were added or moved to 202.1 and subpart 239.76 was added to include cloud computing. Provisions and clauses to be included in the acquisition of commercial items were added to 212.301(f).

SUBPART/ CLAUSE	TITLE	REQUIREMENTS
204.73 (subpart)	**Safeguarding Covered Defense Information and Cyber Incident Reporting.** *Revised – Sept 21, 2015*	▪ Contractors & Subcontractors must safeguard '***Covered***' defense information that resides in or transits through contractor (IT) system. ▪ Must submit to DoD i) incident report, ii) malicious software, and iii) media. ▪ Prescribes: 252.204-7008, -7009, -7012
202.1 (subpart)	**Definitions.** *New Addition – Aug 26, 2015* *Revised - Oct 30, 2015*	▪ Designated subpart as location for definitions: ○ Compromise ○ Cyber Incident ○ Media
239.76 (subpart)	**Cloud Computing.** *New Addition – Aug 26, 2015*	▪ DoD will acquire cloud computing using commercial T&Cs consistent with Federal Law. ▪ Contracts will be awarded to cloud service providers that are granted provisional authorization by DISA. ▪ Prescribes 252.239-7009 & -7010
212.301 (f) (clauses & provisions)	**Solicitation provisions and contract clauses for the acquisition of commercial items.** *Revised – Sept 21, 2015*	▪ Identifies Solicitation clauses and provisions to be included in the acquisition of commercial items. ▪ Includes cybersecurity and safeguards identified in the above clauses.

FIGURE 9. DFARS Clauses

The key requirements of 252.204-7012 are summarized in FIGURE 10. Important requirements from this clause are:

1. Implementation of the clause 'as soon as practical, and no later than December of 2017,
2. Incident reporting within 72 hours to both the DoD and prime contractor,
3. Preservation of the media and capture of the malware if possible. The Cloud Computing provisions follow a similar outline but require that the bidder declare the intent to use cloud computing at the time of the bid. Other arrangements or changes regarding cloud computing must be approved in writing by the contract officer.

DFARS CLAUSE	TITLE	REQUIREMENTS
252.204-7012 (clause)	**Safeguarding Covered Defense Information and Cyber Incident Reporting.** *Revised – Sept 21, 2015* *Revise - Dec 30, 2015*	▪ Contractor will implement information systems security protections on all covered contractor information systems. ▪ Contractor (Offeror) **represents that it will implement security requirements in NIST 800-171 as soon as practical but no later than December 31, 2017.** ▪ Contractor will apply **other information system security measures** when the contractor reasonably determines that [additional] security measures are required. ▪ Contractor **will report, within 72 hours**, incidence report to both the prime contractor & DoD via http://dibnet.dod.mil ▪ Medium Assurance Certificate required ▪ **Preserve and Protect Media Image** ▪ **Submit Malicious code if isolated** ▪ Provide additional information if requested by the government ▪ "Alternative but equal effective" security measures …accepted in writing by an "authorized representative of the DoD CIO will "adjudicate" offeror requests. ▪ **Flow down of DFARS 252.204-7012** is now limited only to subcontracts, "or similar contractual instruments," for 1) operationally critical support or 2) that involve a covered contractor information system

FIGURE 10. Key Requirements of DFARS 252.204-7012

Additional information regarding the DFARS can be obtained at www.i2ComplianceTools.com.

There is another activity the reader should be aware of and fully understand the implications of. The National Archives and Records Administration (NARA) has the responsibility of establishing uniform markings for Controlled Unclassified Information (CUI) that is sensitive and needs to be controlled. As part of their effort, NARA has added a clause to the Federal Acquisition Regulation (FAR) that requires all companies or contractors doing business with the federal government – ANYWHERE - to implement 15 cybersecurity controls to protect information systems that contain Federally Covered Information. On May 16, 2016 the DoD, General Services Administration (GSA), and the National Aeronautics and Space Administration (NASA) issued a final rule to add a new subpart to Title 48 of the Code of Federal Regulations (CFR) containing the FAR. The new Subpart 4.19 "Basic Safeguarding of Covered Contractor Information Systems" prescribes the contract clause 52.204-21 with the same title as the subpart. The effective date is June 15 of 2016.

The required controls selected for 52.204-21 came from the NIST SP 800-171 "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" (June 2015). The FAR requirements and requirements from NIST 800-171 are shown FIGURE 11 below. The requirements are identical except for control (vii) which refers to Federal Contract Information (FCI) as apposed to Controlled Unclassified Information (CUI), and control (ix) that combined three 171 controls as shown. Although 15 (or 17) requirements is a small fraction of the total 109 requirements contained in NIST SP 800-171, they cover 6 of the 14 requirements families as shown in FIGURE 12. Arguably, a large fraction of the effort required to comply with the 6 families and 15 requirements represents a large fraction of the total effort rquired to comply with all of NIST 800-171.

NARA CUI Requirements	
FAR 52.204-21 Specified Requirements	**Corresponding NIST (SP) 800-171 Requirements**
(i) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	3.1.1 Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
(ii) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	3.1.2 Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
(iii) Verify and control/limit connections to and use of external information systems.	3.1.20 Verify and control/limit connections to and use of external information systems.
(iv) Control information posted or processed on publicly accessible information systems.	3.1.22 Control information posted or processed on publicly accessible information systems.
(v) Identify information system users, processes acting on behalf of users, or devices.	3.5.1 Identify information system users, processes acting on behalf of users, or devices.
(vi) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	3.5.2 Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
(vii) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.	3.8.3 Sanitize or destroy information system media containing CUI before disposal or release for reuse.
(viii) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.	3.10.1 Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.
(ix) Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.	3.10.3 Escort visitors and monitor visitor activity. 3.10.4 Maintain audit logs of physical access. 3.10.5 Control and manage physical access devices.
(x) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	3.13.1 Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.
(xi) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	3.13.5 Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
(xii) Identify, report, and correct information and information system flaws in a timely manner.	3.14.1 Identify, report, and correct information and information system flaws in a timely manner.
(xiii) Provide protection from malicious code at appropriate locations within organizational information systems.	3.14.2 Provide protection from malicious code at appropriate locations within organizational information systems.
(xiv) Update malicious code protection mechanisms when new releases are available.	3.14.4 Update malicious code protection mechanisms when new releases are available.
(xv) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.	3.14.5 Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

FIGURE 11.FAR 2016 CUI Requirement

When NIST published 800-171 in June of 2015, they anticipated that all federal contractors would need to comply with the standard (FIGURE 13). Although not all of 800-171 is required, it appears that the intent is to have, in the relatively near future, all federal contractors complying with the standard. The full implementation of NIST 800-171 in DoD was postponed to December of 2017 (although contracting officers are including the DFARS clause in many procurments). That well may be the time horizon for all federal contractors.

Security Families in NIST (SP) 800-171	
AC - Access Control (3.1)	
AT - Awareness & Training (3.2)	
AU - Audit & Accountability (3.3)	
CM - Configuration Management (3.4)	
IA - Identification & Authentication (3.5)	
IR - Incident Response (3.6)	
MA - Maintenance (3.7)	
MP - Media Protection (3.8)	
PS - Personnel Security (3.9)	
PE - Physical Protection (3.10)	
RA - Risk Assessment (3.11)	
CA - Security Assessment (3.12)	
SC - System & Communications Protection (3.13)	
SI - System & Information Integrity (3.14)	
Included in FAR	*Not Included in FAR*

FIGURE 12: Security Families Included in FAR 52.204-21

"Executive Order 13556, Controlled Unclassified Information, November 4, 2010, established the CUI Program and designated the National Archives and Record Administration (NARA) as its Executive Agent to implement the Order and to oversee agency actions to ensure compliance with the Order. Regarding contractors, the CUI Executive Agent anticipates establishing a single Federal Acquisition Regulation (FAR) clause in 2016 to apply the requirements of NIST Special Publication 800-171 to the contractor environment as well as to determine oversight responsibilities and requirements. The CUI Executive Agent also addresses its oversight of federal agencies in the proposed regulation for incorporation into the Code of Federal Regulations. Approaches to oversight will be determined through the uniform CUI FAR clause, future understandings, and any agreements between federal agencies and their nonfederal information-sharing partners."

--Special Publication NIST 800-171, page 15

FIGURE 13: NIST Statement on Cybersecurity Standard for Federal Contractors

FIGURE 14 provides a perspective for anyone who might question the relative severity of the NIST (SP) 800-171 requirements and/or referenced controls. As can be seen from the graphic, the requirements imposed are 'low' when compared to other baselines and are clearly meant to be an entry level security profile.

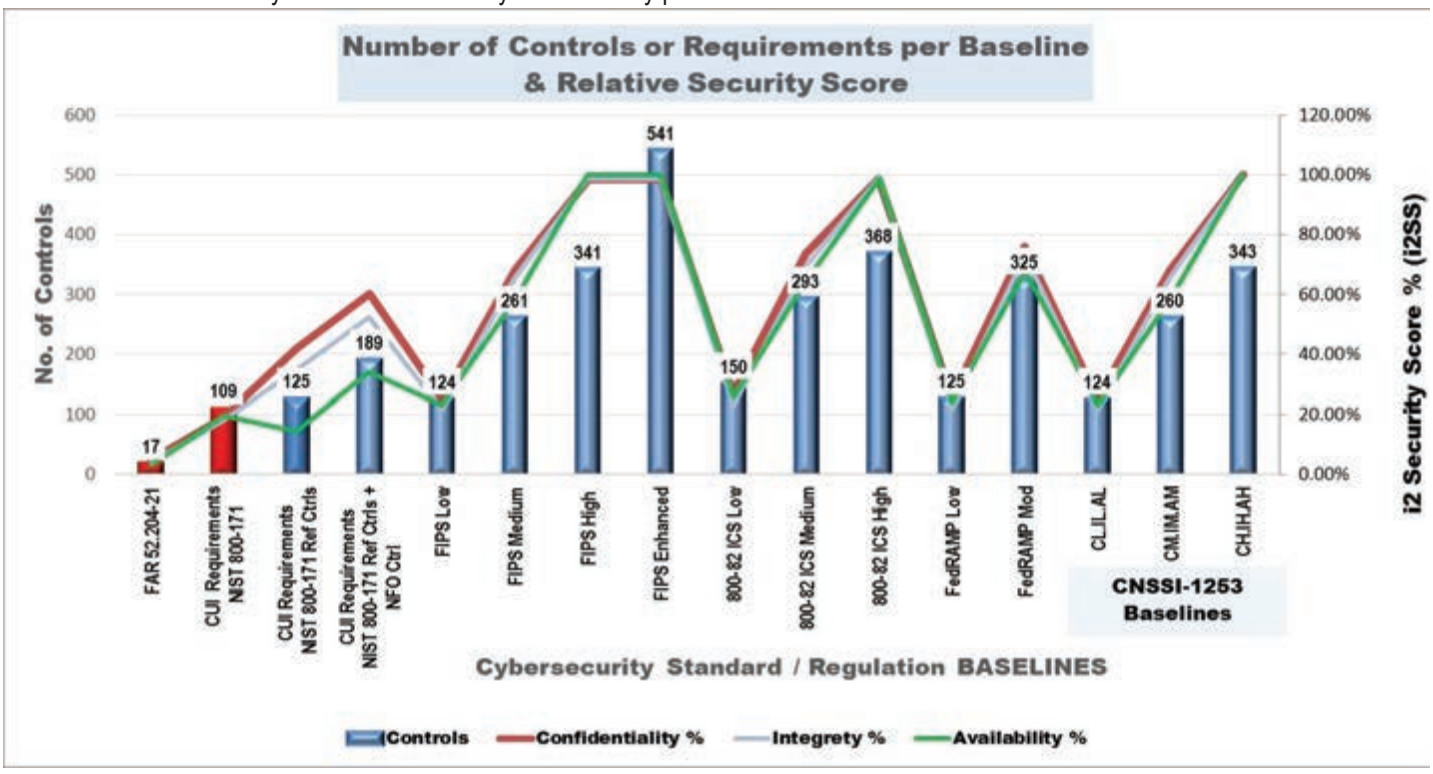

FIGURE 14: The NIST SP 800-171 Baseline Compared to Other Baselines

RESOURCE, TOOLS, & SUPPORT OPTIONS

OPTIONS
Resources
1. DHS, NIST, GOVERNMENT
2. DIB ISAC (Defense Industrial Base, Information Sharing & Analysis Center
3. The i2 Cyber Compliance Center (C3 or the Cube)
Tools
4. Spreadsheet & Docs
5. CSET (Cyber Security Evaluation Tool).
6. The i2ACT-800

FIGURE 15:Resources and Options

Resources, tools, and support options available to organizations who need, or want, to come into compliance with cybersecurity standards are not plentiful. IT consultants and service firms represent a traditional solution. However, not all service companies will have the understanding or experience in the cybersecurity domain, nor an understanding of the threats. As seen in FIGURE 15 the government provides training material and tools such as the Cyber Security Evaluation Tool (CSET). These are all very good resources, but do not necessarily achieve system compliance in the shortest period of time, nor with the greatest accuracy and fidelity. Nonetheless, they are an excellent library of resources.

The National Infrastructure Protection Plan (NIPP) calls for the establishment of Information Sharing and Analysis Centers (ISACs) in each of the industrial segments in the critical infrastructure. For defense companies, the Defense Industrial Base (DIB) ISAC is a great resource and has established both an information sharing capability for members and also developed the Cyber Verify™ process to certify contractors as being in compliance.

The firm publishing this white paper, Imprimis, Inc., has established the Cyber Compliance Center (C3 or the Cube) to support organizations in a cost effective manner. The Cube is a center that supports remotely by phone, VTC, and remote access any firm requiring assistance. This is considered a cost effective option to consulting firms and supports the companies as they take charge of their system compliance.

The most common practice today for assessment and compliance efforts are spreadsheets and documents maintained in a file sharing environment. The Department of Homeland Security (DHS) has developed an excellent reference tool, CSET, that can support the assessment and compliance process. CSET, however, is less than ideal for managing the assessment and compliance process. It also does not support NIST 800-171 at this time.

Finally, there is a tool made specifically for the purpose of supporting assessment and compliance efforts that has been developed by Imprimis, Inc. (i2), the i2 Assessment & Compliance Tool or the i2ACT. There are two tools pertaining to the NIST 800 series of standards, the i2ACT-800 PRO and the i2ACT-800s. The full model (or PRO) contains full capability for all organizations. It contains over 2 dozen pre-configured baselines including all of the CSNSSI-1253 baselines. It supports risk categorization and tailoring and allows the naming of new baselines. It organizes all supporting material and retains these documents as part of the database. The i2ACT-800s is specifically designed for NIST SP 800-171.

INTRODUCING THE i2ACT

i2 has developed Assessment and Compliance Tools, known as the i2ACT suite. These intelligent tools allow you to easily navigate the regulations pertaining to your industry, document your progress, and ensure your team's preparedness for internal and external audit successes.

Of note, the i2ACT-800 has been selected by the DIB ISAC as the tool of choice in assessing compliance with the NIST standards. Another organization that understands the importance of cybersecurity and the application of standards is the Digital Design and Manufacturing Innovation Institute (DMDII). The DMDII is the United States' flagship research institute for

applying cutting-edge digital technologies to reduce the time and cost of manufacturing, strengthen the capabilities of the supply chain, and reduce acquisition costs. They understand that none of this is possible without securing the cyber domain. The University of Illinois Laboratories (UI Labs) were selected by the federal government to be a leading member of the National Network for Manufacturing Innovation (NNMI) and they, in turn, selected i2 to perform an evaluation of the effectiveness and cost of applying the DFARS and to make recommendations regarding effective cybersecurity baselines for manufacturing.

WHAT IS THE i2ACT-800?

The i2ACT-800 tools are purpose-built cybersecurity assessment and compliance tools designed for the security architecture developed by NIST contained in the Special Publication 800 series in response to the requirements defined in the Federal Information System Management Act (FISMA). This tool includes all security controls contained in NIST SP 800-53 and all security requirements contained in NIST SP 800-171. The tools fully support cyber requirements specified in the DFARS 204.73, the FAR 4.19 clause 52.204-21, the Federal Information Processing Standards (FIPS), CNSSI-1253, and supports the RMF adopted by the DoD as a replacement for the DoD Information Assurance Certification and Accreditation Process (DIACAP).

The i2ACT-800 is user friendly and provides an overview of the entire RMF process. It includes a complete reference system and provides simple, intuitive assessment forms and complete reports. In addition, the i2ACT-800 includes:

1. A full user manual.
2. A user website with video training, instructions, briefings, and support material.
3. Compliance questions to help the user better understand each control
4. A ticketing system and help desk for i2ACT-800 users.
5. Access time with the Imprimis, Inc. Cyber Compliance Center (C3 or the Cube) providing cyber compliance expertise to users of the i2ACT tools.

HOW DOES THE i2ACT WORK?

•THE ARCHITECTURE

The i2ACT-800 is a compliance tool for the NIST Special Publication 800 series built with the use of a relational database. The database used is Microsoft Access which is installed in Runtime 2013 version so no additional software is required by the user. However, as shown in FIGURE 16, the i2ACT-800 is actually split into 2 databases: the front end which is the user interface and the back end which contains the user's data and information. The user can create a new database or connect to an existing database. The user can connect and reconnect at will.

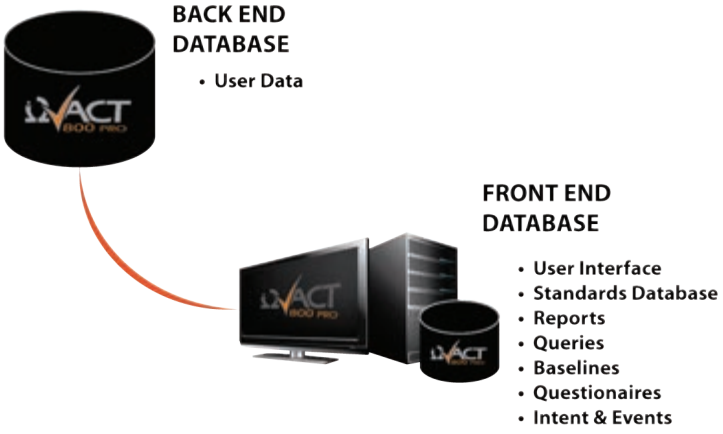

FIGURE 16: i2ACT 800 Database Structure

This feature allows the user to create their own database, connect to and work on a number of separate projects, or join a joint project that can have up to 20 users working on the same database (FIGURE 17). It also allows the project lead to check the status of any project at any time. Collaboration of several people with varied backgrounds is essential for compliance teams.

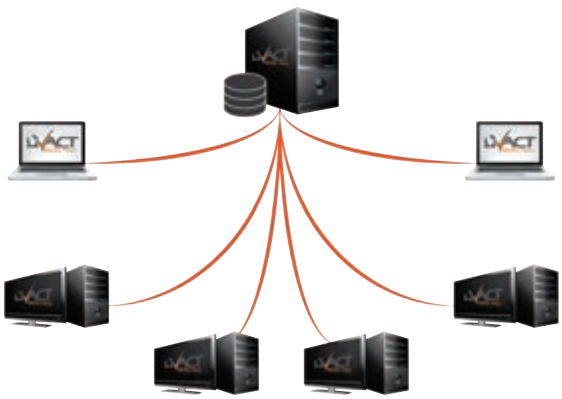

FIGURE 17: Collaboration with Compliance Team

The i2 team has done significant analysis on the volume of data that might be collected during a compliance review and could not establish a scenario where the Access database was not adequate by a sizable margin. Nonetheless, the two-part construction allows the front end database to be connected to a Microsoft SQL Server database which can handle any volume of data needed

for the compliance process.

The Runtime version of Access is installed during the installation of the i2ACT-800 so the user does not have to have Access on their computer. Updates will be delivered to the front end database so back end databases will not be disturbed. Any changes in the standards or regulations will be updated directly to the front end as will improvements and changes in capability of the tool. All information recorded in the user or back end database, including all attachments, will remain in the database when stored or archived. So if an audit occurs 10 years later, all information will be contained within the stored database suffering no lost files.

•CONTENT AND DASHBOARDS

The Dashboard of the i2ACT-800 PRO is divided into four major sections: References, Risk Categorization & Baselining, Assessment and Reports, and Data Management (FIGURE 18). The 'About' tab provides version and license information and access to technical support and the user's manual. The Reference section contains all of the controls and enhancements contained in the NIST SP 800-53 and all requirements in NIST SP 800-171. The reference section allows the user to search all controls and requirements and provides definitions and navigational aids.

FIGURE 18: The i2ACT 800 PRO Dashboard

The second section supports risk categorization and baseline selection and tailoring of the selected or specified baseline. Risk categorization and baselining are supported for both NIST SP 800-53 and NIST SP 800-171. FIPS, CNSS, DFARS, and FAR specified baselines are supported. Most frequently, a minimum baseline is specified by the government or parent organization, but the organization may modify the specified baselines as required. After the baseline is established, the assessment begins. Each control or requirement is addressed during the process to determine if the system and organization comply with the stated security requirements. Any remediation requirements are addressed in the Plan of Actions and Milestones (POA&M). There are numerous reports available in i2ACT-800 PRO and i2ACT-800s supporting program management and actions as well as reports suitable for submitting to contract officers or prime contractors. The final section is data and file management. Data is collected on the organizations involved in the assessment (both the subject of the assessment and the firm performing the assessment), the baseline(s) developed and used, and the assessment and remediation information. These are stored in the 'back end' databases and organized through the dashboard.

The i2ACT-800s was developed specifically for addressing compliance with NIST SP 800-171 (FIGURE 19). It is an ideal tool for managing the process of complying with DFARS and the new FAR requirements recognizing that full compliance with NIST 800-171 soon to be a requirement. The organization of the tool and functionality are the same as the i2ACT-800 PRO but does not support all of the NIST SP 800-53 controls, the full RMF, nor FIPS or CNSS baselines. It does include the NIST SP 800-53 controls referenced by the requirements in NIST SP 800-171.

FIGURE 19: The i2ACT-800s Dashboard

•PROCESS OVERVIEW

The process flow for cybersecurity assessment and compliance is shown in FIGURE 20. The first step is to perform the risk categorization of the system and select and tailor the appropriate baseline of controls or requirements, or both. Each control systematically steps through assessing and documenting the state of compliance. Remediation requirements are determined as each control is assessed and then again at the end of the process. The assessment is then ended and remediation initiated. Documentation is updated to note the remediation that has occurred. Then the documentation is maintained as a critical corporate document, most likely as part of a configuration control function, and updates are added as needed until the next assessment is initiated. Information describing full compliance or information describing shortcomings are stored in the database. Attachments containing system diagrams, vulnerability scans, policies, screenshots of device configurations, and other descriptive information are included as attachments.

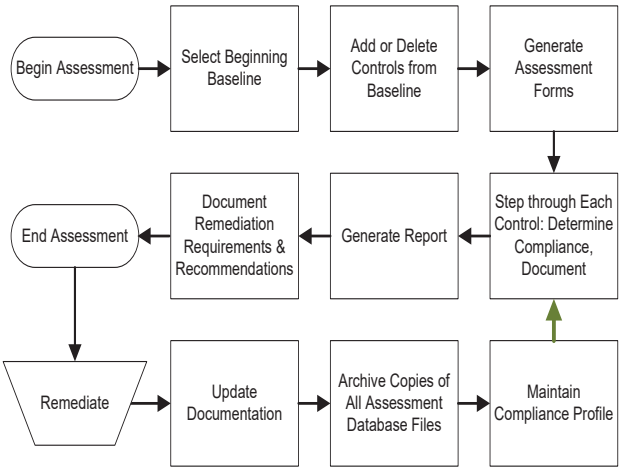

FIGURE 20: Continuous Assessment Flow

•RISK CATEGORIZATION, SELECTING & TAILORING A BASELINE

First, some definition; what are baselines and overlays? A "baseline" is a set of security controls selected for a particular system or application. An "overlay" is the addition or deletion of controls from an existing baseline resulting in a new baseline. So DFARS Clause 252.204-7012 specifies a number of controls from NIST SP 800-171 with which contractors must comply. This is the DFARS baseline. If a user adds additional controls needed for their system, the controls added by the user would be an overlay. The combined result is a new baseline which the user would name.

The first step in the process is to categorize the system. This process is defined in FIPS 199 (FIGURE 21). The impact on CIA are defined. If this process is for a FIPS covered system, the high water mark is used. In other words, the highest score defines the baseline used. The CNSS process actually defines a baseline for CIA. This process defines the baseline which, in turn, is entered into the tailoring process.

FIGURE 21 : Risk Categorization

The i2ACT-800 PRO provides a number of existing baselines including DFARS, FIPS low, FIPS mid, FIPS high, FIPS enhanced, Industrial Control Systems (ICS) low, ICS mid, ICS high, all CNSSI-1253 baselines, and the NIST SP 800-171 required for federal contractors (FIGURE 22). Over two dozen existing baselines are provided. These options are provided to the user during the initial stages of baseline development. A single baseline can be selected, combinations can be selected, or the user can start without an existing baseline and build their own. The RMF 800-37 will support the user in their efforts to establish an initial baseline of requirements that most accurately reflect their Information System Security needs. The baseline is often prescribed by regulation or contractual specification. (Nothing can be removed from a baseline during the tailoring process that is prescribed by regulation or contract.)

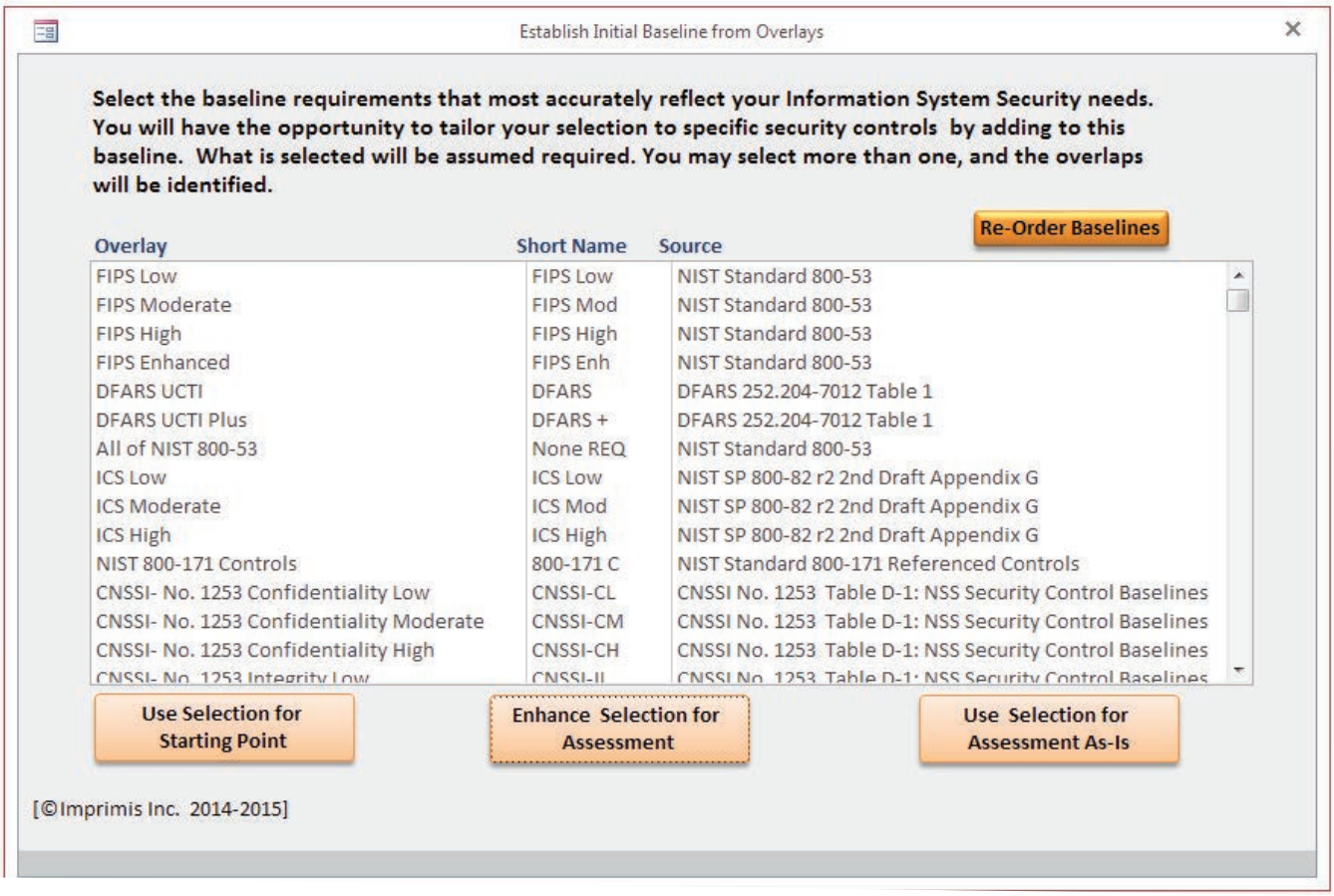

FIGURE 22: i2ACT-800 Pre-Loaded Baselines

The user may then decide to use a predefined baseline based on the risk categorization and stop the tailoring process at that time. However, the tool allows the user to continue developing a baseline that they feel is appropriate for their organization. This may have to do with the nature of the business operations or may reflect multiple customers specifying multiple standards or baselines. An example of process differences is the use of ICS for manufacturing, power distribution and management, building control, or a variety of other end uses. All DFARS and FAR requirements optimize the confidentiality of information. However, in ICS environments, availability and integrity are higher priorities in most cases than confidentiality. As a result, the user may want to add controls that enhance availability.

As a result, the i2ACT-800 was designed to allow the user to select a single existing baseline or combinations of baselines (e.g., DFARS and FIPS low) and to set other controls as 'required' or 'desired' (FIGURE 23). The latter indicator is useful when an organization wants to enhance their security profile and manage the improvements in their system. The DFARS require the user to perform a very thoughtful process in selecting the controls in the final baseline. Specifically, in DFARS 252.204-7012 states ***"Contractor will apply other information system security measures when the contractor reasonably determines that [additional] security measures are required".***

The implementation guidelines for these standards call for an investigation into incidences, particularly those resulting in the loss of sensitive information, to see if the sytem and organization where in fact in compliance with the regulations and the standards. The government may not do periodic audits or inspections of the systems, but each proposal calls for the principals of the company or organization to represent and certify that the organization is in compliance with the requirement. In those instances where the organization was not in compliance when it was breached, serious repercussions can result from falsely representing compliance. This is a serious matter and should be treated as such. Selecting or developing a security baseline with accompanying rationale and achieving compliance, verifying compliance (internally or externally) is the cheapest form of cyber insurance the organization can buy.

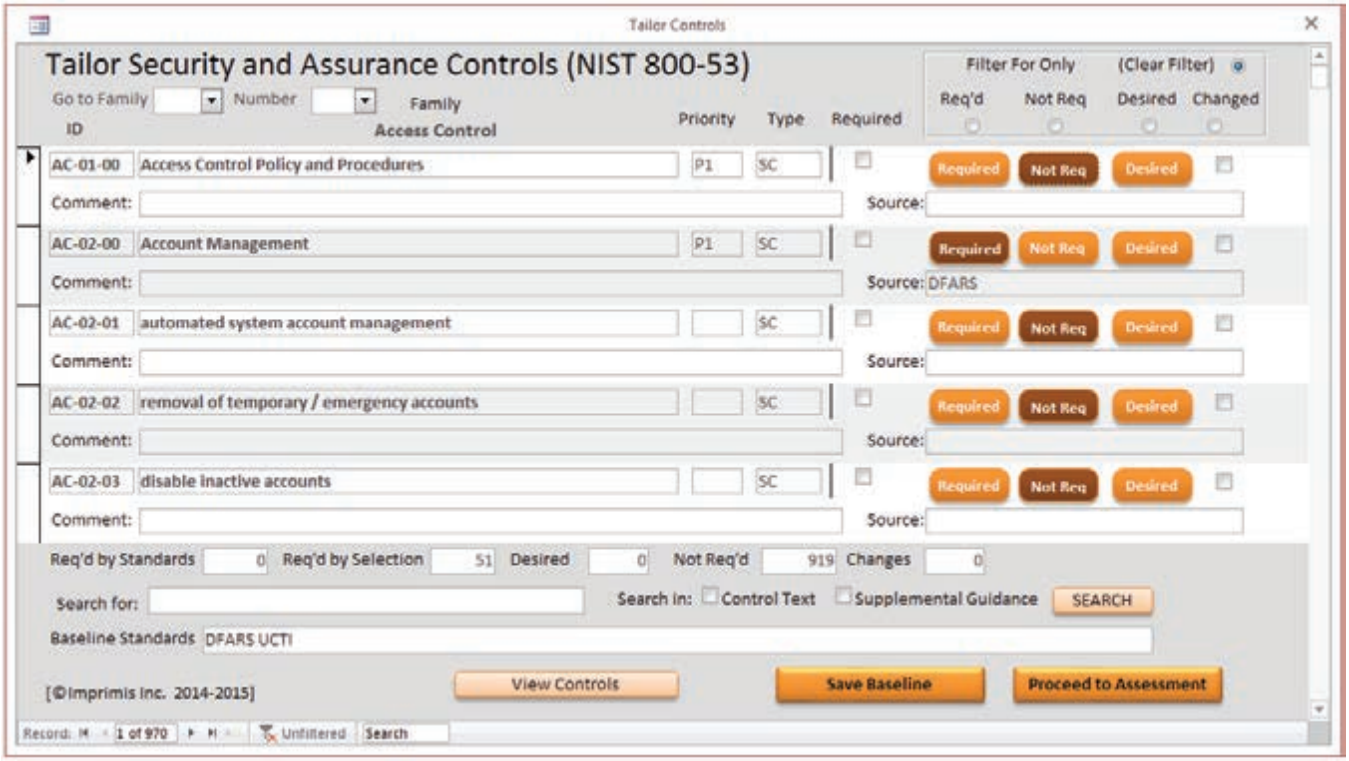

FIGURE 23: Tailor Baseline Specific to Organization Needs

It is also important that as all organizations mature, they improve their security profile or baseline over time. New controls can be added to the baseline with each assessment, or if experience dictates, additional controls can be added when determined necessary after an incident. Thus, the first baseline an organization develops is a starting point and changes over time are necessary and these changes are to be expected. Once a baseline is tailored for an organization, the i2ACT-800 provides the ability to name and save the resulting baseline as shown in FIGURE 24. It also allows the user to export the baseline and could send it to other users within the organization as guidance for cybersecurity.

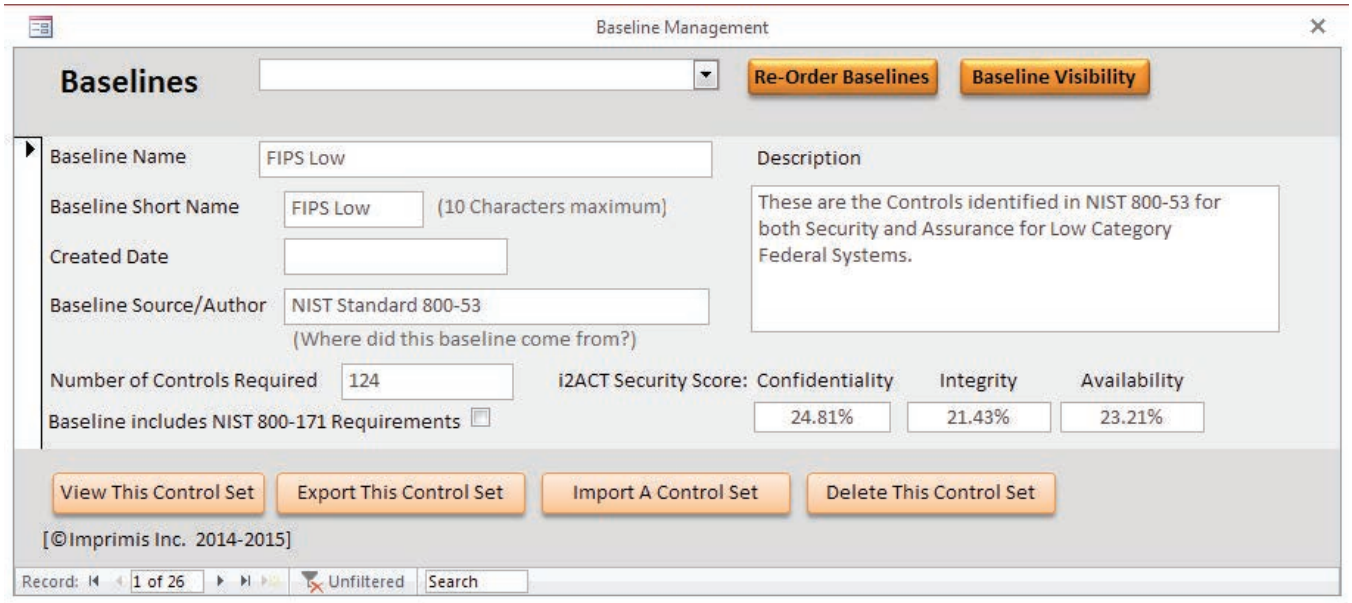

FIGURE 24: Saving and Managing Tailored Baselines

•THE ASSESSMENT

The assessment form for the NIST 800-53 RMF and the NIST 800-171 are the same in structure and very similar in content. In the NIST 800-53, each control is identified and supplemental information is provided. FIGURE 25 shows the detailed assessment

page. Tabs are provided that contain not only supplemental guidance but any special guidance provided, questions that pertain to the control, a description of the intent and suggested evidence for each control, and a remediation tab that captures any actions required for full compliance. Once the desired set of controls is established, each control is evaluated for the company's compliance with each item. The short version of the assessment page is shown in FIGURE 26 and allows the user to examine the assessments without all other data being displayed.

FIGURE 25: Detailed Assessment Page for NIST 800-53

Each control should have comments and documentation (when possible) to support claims of compliance. The documentation for each control needs to be detailed and pointed, clearly showing compliance with each and every item contained within the control. Attachments should be included to show such items as policies, minutes of meetings, network diagrams, screenshots of settings, pictures of physical controls, and any other supporting documentation needed. The physical location, URL, and other locators should be included so that anyone following the internal assessor will know where to find the article if necessary. The one person that will have to follow the internal assessor at some time is the independent auditor. The auditor will need to verify the information contained in the assessment form.

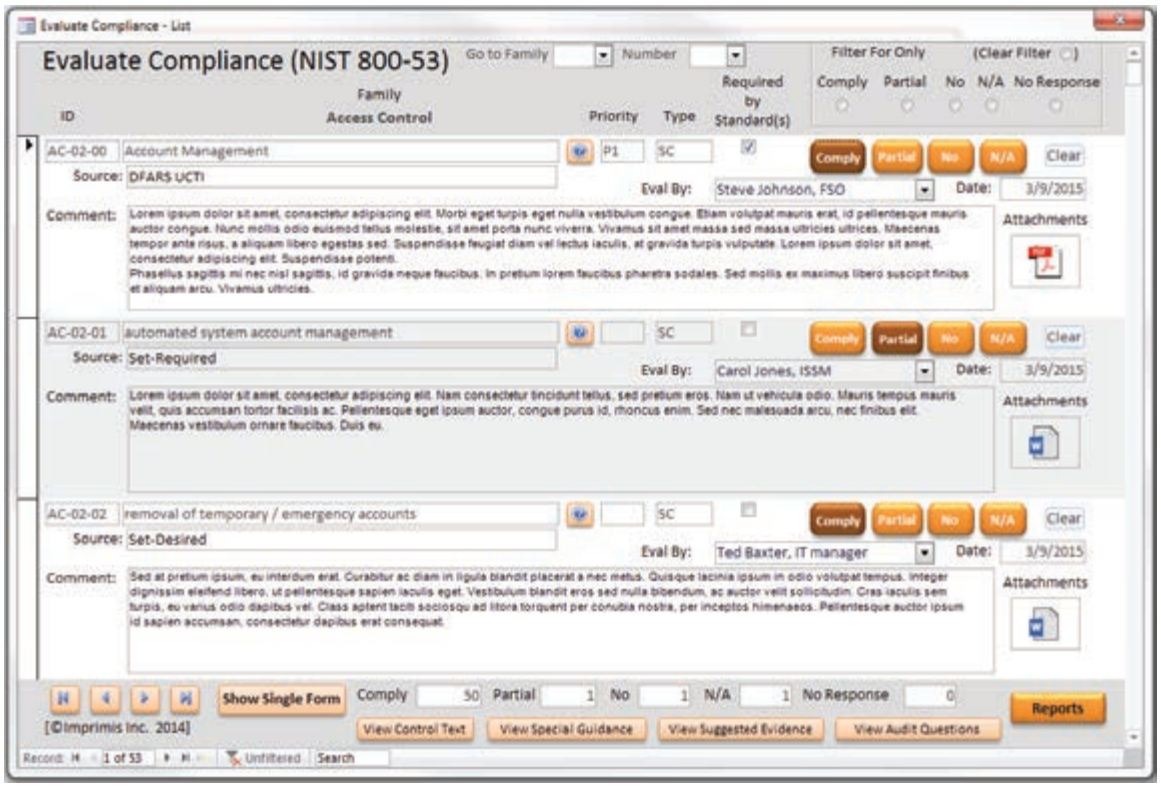

FIGURE 26: Assessment Forms Consolidated

The remediation tab is shown in FIGURE 27. During the assessment, the 'comments' window captures the current description of the state of compliance with enough specifics to convincingly describe how compliance is met or achieved. Documents can be attached that support the conclusion. These documents can contain written documents such as policies and procedures, screen

shots of settings, system diagrams and other pertinent information. One major advantage of the i2ACT-800 is that it contains full copies of these documents that remain in the database even after archiving. There will be no issue with broken links or lost documents. Questions are included in the i2ACT-800 as an aid to those performing the internal assessment.

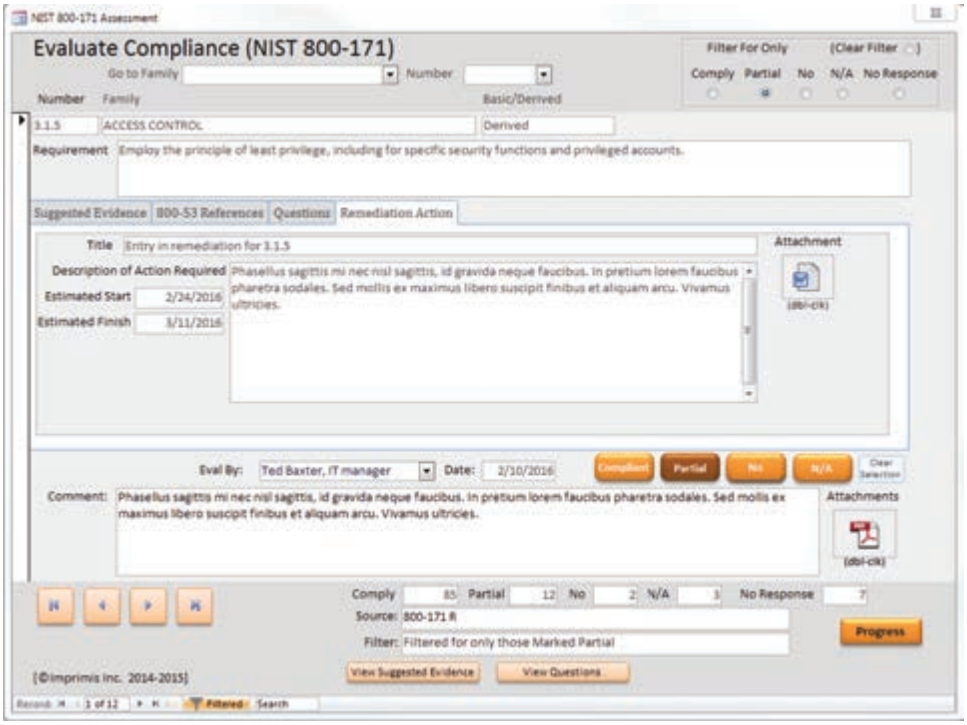

FIGURE 27 : Remediation Tab

Questions help guide the process and focus the thinking on compliance indicators. They also prepare staff for questions that will come from an outside auditor. These questions have been derived from CSET. i2 intends to continue to add ”frequently asked questions” and other information volunteered by participating organizations. However, one caveat needs to be made very clear. Although questions are useful, ANSWERING QUESTIONS DOES NOT EQUATE TO, INSURE, OR OTHERWISE GUARANTEE COMPLIANCE. Only meeting the intent and complying with all details within a control, establishing compliance with the control, and doing so for all controls in the selected and qualified baseline will yield system cybersecurity compliance.

The assessment forms for the NIST 800-171 compliance assessment are shown in FIGURE 28 and are very similar to the NIST 800-53 forms described above. However, NIST 800-171 specifies requirements rather than controls, but does reference a number of NIST 800-53 controls. So the assessment form provided within the i2ACT-800 provides both the requirement and referenced controls. The support tabs also include suggested evidence, questions, and a remediation tab.

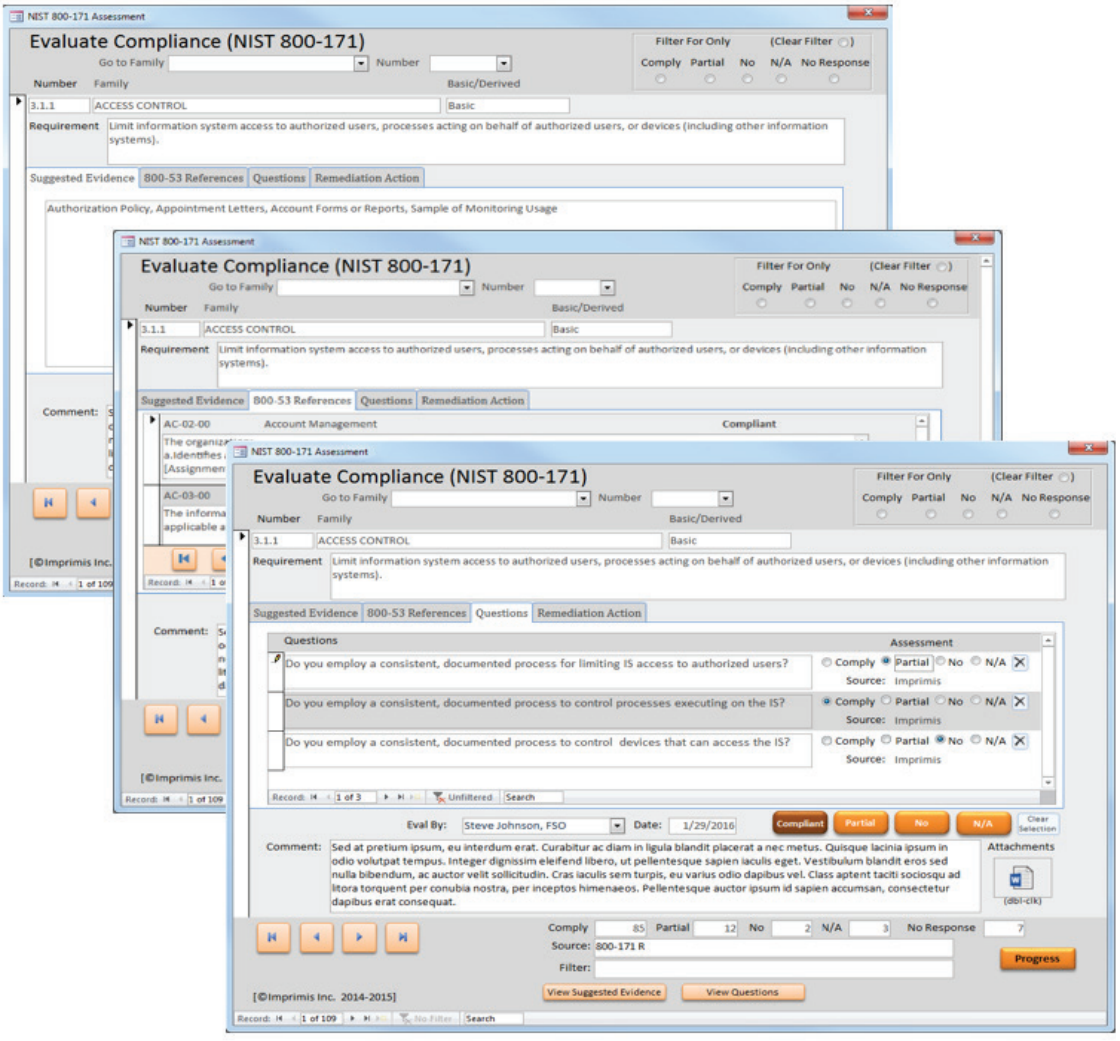

FIGURE 28: The i2ACT 800s Assessment Forms and Tabs

•REPORTS & PLANS

The information that is captured during the assessment is available for publication in a variety of reports which include assessment reports, completed questionnaires, and remediation reports. The report manager allows the user to compose any report that they may wish to publish. FIGURE 29 provides a screen shot of the report manager within the i2ACT-800. Reports of assessments performed for a NIST SP 800-53 standard, NIST SP 800-171, or the NIST SP 800-171 with the referenced controls from NIST SP 800-53.

FIGURE 29: Report Manager Screen

Each report can contain a cover page with organizational information, a summary at the beginning of the report or at the end, and can contain all information items or only the ones the user selects. Reports containing all the data may be published and summary reports can be selected as well. Controls, requirements, comments, questionnaires, and remediation reports at the user's fingertips.

One of the key features is the ability to not only publish a remediation plan, but to establish a PO&AM. All of the information contained in the remediation tab for each control and requirement is exportable in XML and spreadsheet and can be used in Microsoft Project (FIGURE 30) or another spreadsheet schedule program (FIGURE 31). This feature provides management control over the remediation process and the schedule for achieving full compliance. It also allows management to have full oversight of the process and the status of the remediation activity. It is a very strong tool for internal use, but is also useful for managing IT consultants who may have been retained to make modifications required for compliance.

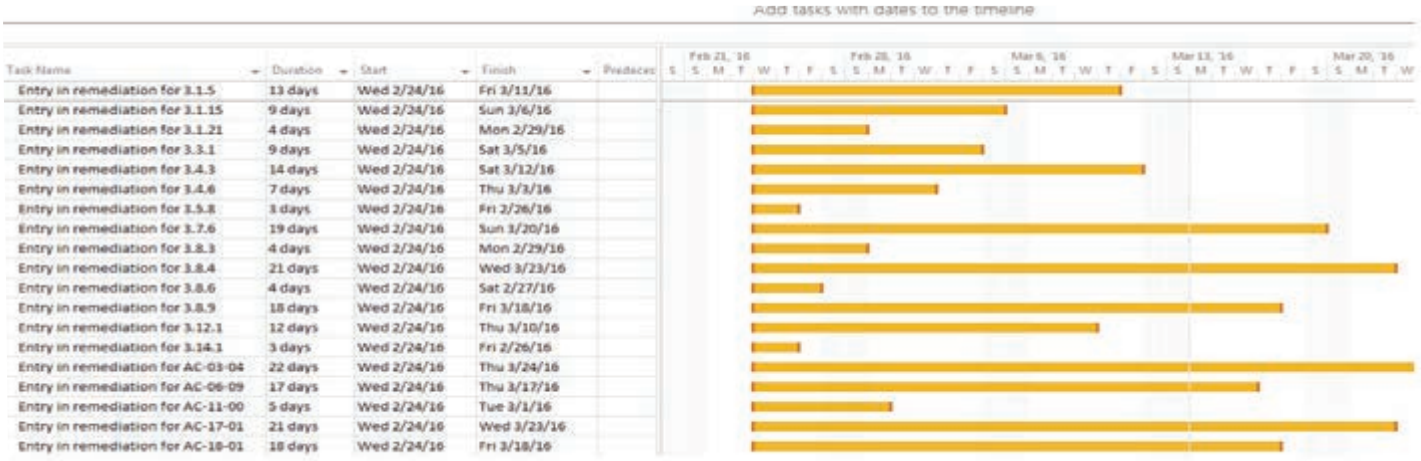

FIGURE 30: Remediation POA&M into Microsoft Project

These tools take the uncertainty out of the assessment and compliance process and empower each organization to have full control over the process

FIGURE 31: POA&M Schedule Exports to Spreadsheets

•MULTI-SITE, MULTI-ORGANIZATIONAL ROLLUP

Imprimis has recently added a rollup feature to the i2ACT family of products. This tool is used when an organization may have multiple sites and networks, or a prime contractor must ensure that all subcontractors are in compliance. If each of the subcontractors or networks completes the assessment and provides a copy of the database to the prime or parent organization, these can be rolled up into a single report on the status of all sub elements and provides a drill-down capability to examine selected areas of concern.

The control panel of the i2ACT Rollup tool is shown in FIGURE 32. The control panel allows for the import and export of i2ACT-800 databases, the management of the databases received individually and in compilation. Then the aggregate information can be viewed in summary or by individual company or network, or each requirement or control can be examined to determine collective performance.

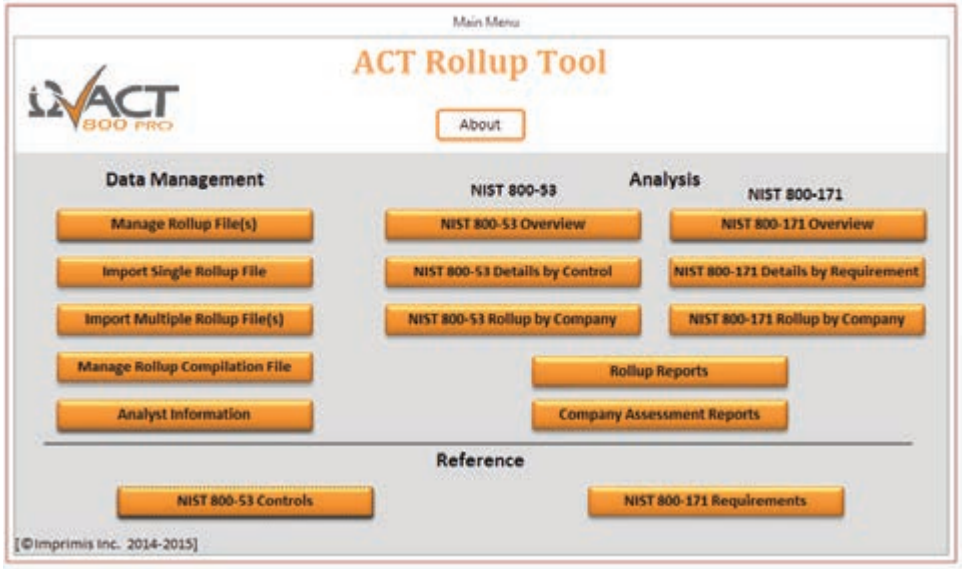

FIGURE 32: i2ACT Rollup Dashboard

The Rollup tool supports analysis with respect to NIST 800-53 and NIST 800-171 as shown in FIGURE 33. The user can choose between compliance summaries of each company or subnet or by control and/or requirement. The individual reports on each assessment can be pulled up for detailed examination. Also, dating files for individual companies will allow trend analysis of the individual company. This feature can also be used by an individual organization to track improvements or trends.

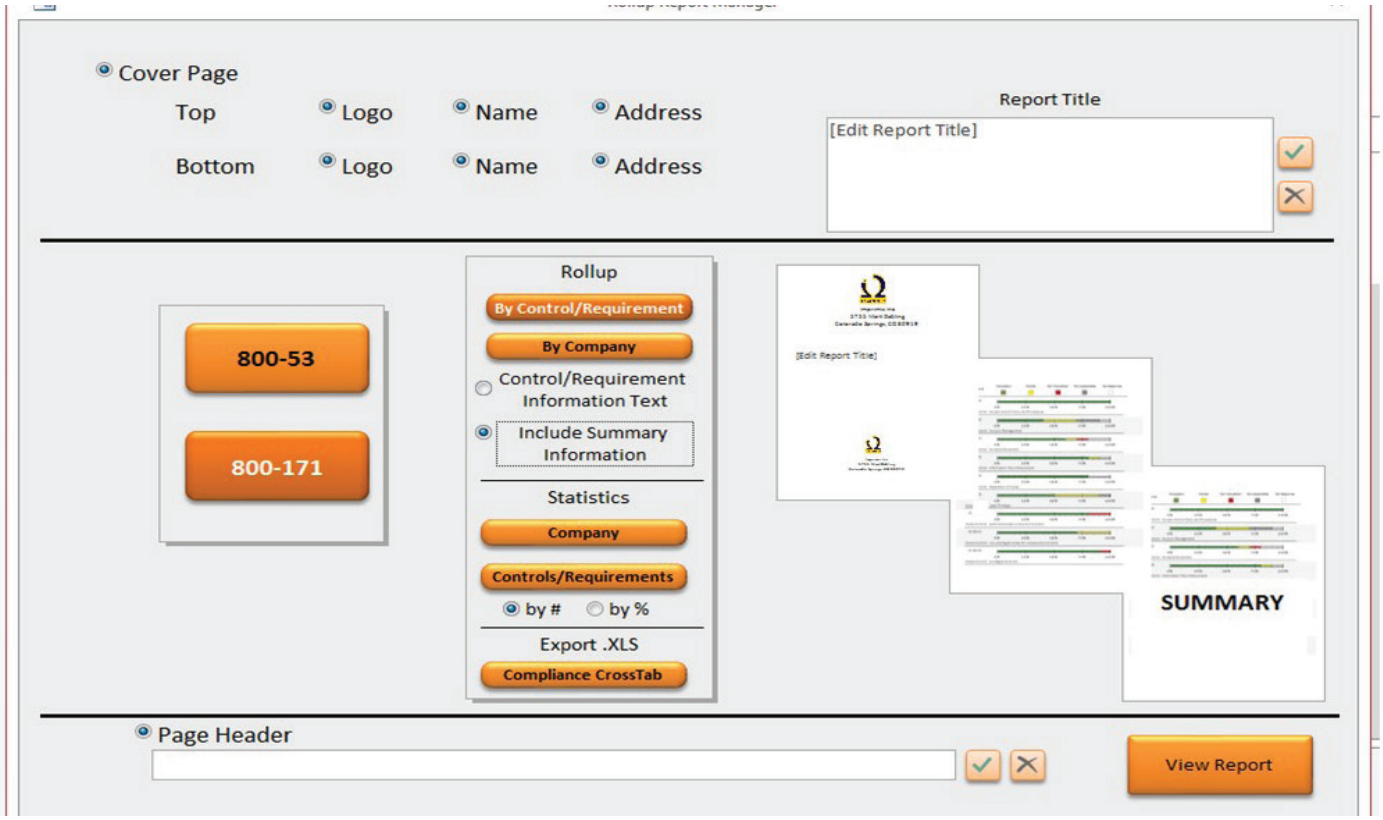

FIGURE 33: Rollup Report Manager

Thus, the Rollup tool provides a:

- Summary view of all subcontractors or subnets,
- Detailed examination of individual assessments or 'drill-down' capability,
- Detailed analysis by control or requirement, and
- Trend analysis for individual organizations or aggregate performance.

•THE i2 CYBER COMPLIANCE CENTER

The i2ACT Suite was designed to support and guide companies and organizations in performing their own assessment and establishing a remediation plan. The tool focuses their efforts on the right tasks and both saves time and helps avoid mistakes in execution from the lack of experience or understanding. Even if an outside consulting firm is performing the assessment, their labor costs should be greatly reduced with the use of the tool.

However, questions do arise during the assessment regarding evidence, approaches for satisfying the control or requirement, procedural questions, organizational questions, and many more. In addition, all companies and organizations want to save expenditures and control costs, especially small businesses. Understanding these needs, i2 developed the Cube (FIGURE 34).

Cube time is allocated to each user when they subscribe to one of the i2ACT products. Additional services can be purchased in quarter hour increments. The staff can answer questions asked by a user or can perform far more extensive services.

The services offered through the Cube cover the spectrum required for cybersecurity compliance programs. Helping clients through risk categorization, controls selection and baseline development, assessment, remediation, and preparation for red team audit. The support is provided via VTC, remote scans, and telephonic discussions.

FIGURE 34: The Cyber Compliance Center

•FEATURES AND BENEFITS OF THE i2ACT-800

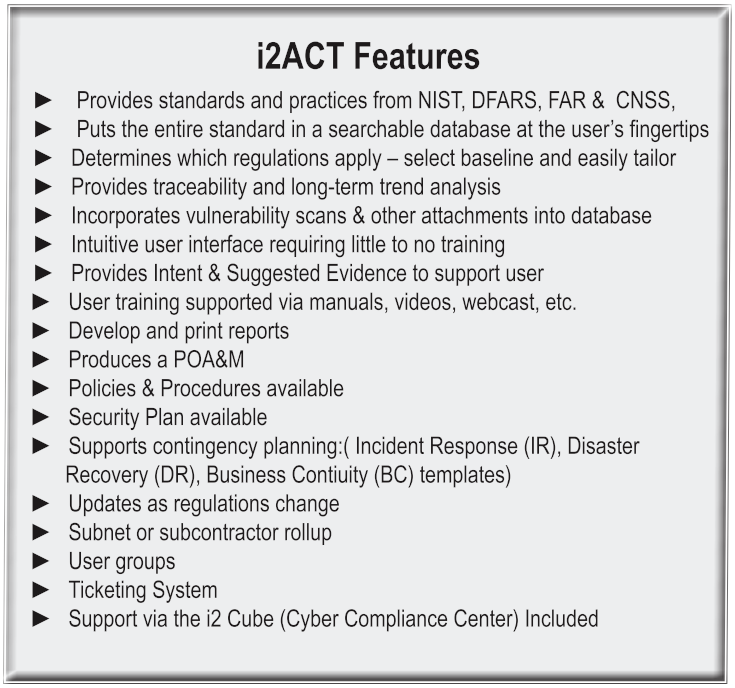

FIGURE 35: i2ACT Features

So how does the i2ACT-800 help? There are many ways the use of the tool reduces the work required from the business staff. All of these attributes save time and improve the end product which is system security. And heuristics apply – each year will be better than the last. If new team members are brought into the process, the completed i2ACT-800 forms will be a great training aid. The initial productivity increase is a great cost and pain saver, but the benefits continue to increase as the tool is used.

There are numerous features in the i2ACT-800 PRO and the i2ACT-800s. These features are summarized in FIGURE 35 and are growing at a rapid rate. They include providing a database of the standards that is easisly navigated by the user and one that can be searched by the user. It provides baselines and allows tailoring of baselines. It comes with templates for policies and procedures and business continuity plans, and many more. User feedback is used to develop features that serve the end users in the best way possible Collectively, these features contribute to a number of functional attributes as summarized in FIGURE 36. And these yield the user benefits shown in FIGURE 37 .

FIGURE 36: i2ACT Functional Benefits

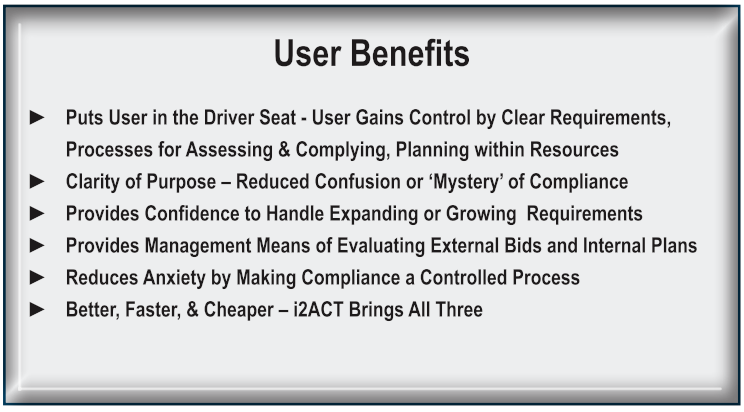

FIGURE 37: i2ACT User Benefits

CASE STUDIES

APPROACH AND ASSUMPTIONS

The i2ACT-800 was developed by i2 out of necessity. Internalizing, understanding, organizing and ultimately complying with the controls used in NIST SP 800 was an overwhelming task – and we are an IT company! Our language has changed - the way we frame requirements reflect the family of controls, and all of the IT staff and many of the others have adopted behavior that reflects the need for security in the cyber domain. Thus, the tool was born out of necessity and that is one of the major reasons it is so effective and valuable to users.

A huge benefit realized is the **productivity** afforded by the tool. But other important benefits should not be ignored. **Focus:** working on the productive tasks will yield the best results. **Quality**: training, explanations and understanding will result in much better solutions. And all of this results in improved security.

The productivity is significant.

To illustrate the savings, i2 has developed three case studies to illustrate the productivity and savings. The three case studies include:

1. A mid-level organization that may range from a few dozen employees to hundreds. The assessment is performed by a team of 5 or 6 staff.
2. A small organization that has one individual responsible for the assessment and compliance possibly assisted by a technical writer or junior staff member for the purpose of documentation.
3. An enterprise organization with multiple networks within the organization.

The RMF requires a team approach with all major segments of the organization represented and the i2ACT-800 supports this collaborative process. For the purpose of the analysis, we used the RMF, NIST SP 800-37, as guidance with regard to the personnel. As discussed above, these include.

1. authorizing officials;
2. chief information officers;
3. senior information security officers;
4. enterprise/information security architects;
5. information system owners/program managers;
6. information owners/stewards;
7. information system security officers;
8. information system security engineers;
9. information system developers and integrators;
10. system administrators;
11. contracting officers; and
12. users.

The full list would only apply to large enterprises as smaller company or organizations would have fewer requirements and would have their personnel serve multiple functions. As a result, the case studies presented here assume the following **staff positions.**

1. Management / Task Lead
2. Senior IT Network Engineer
3. Security Engineer
4. Facility Security Officer
5. Human Resource / Training Lead
6. Technical Writer, Documentation Manager

We identified the **tasks** that needed to be completed in time for an audit (FIGURE 38), and identified the personnel that needed to be involved per the RMF.

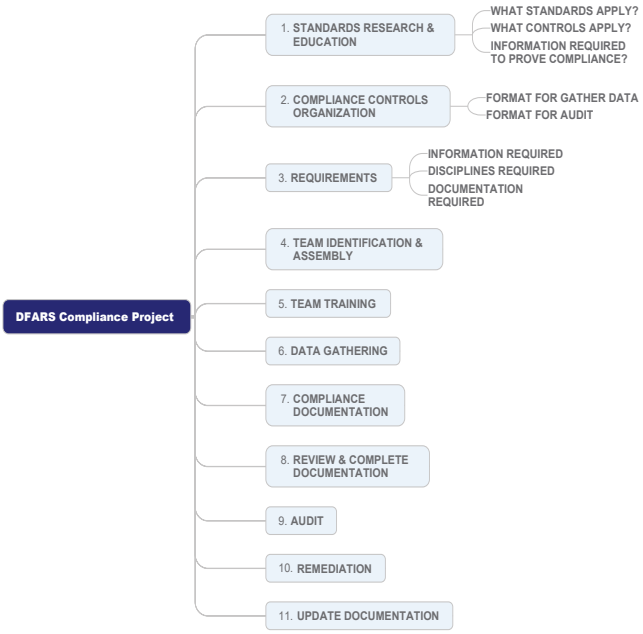

FIGURE 38: Compliance Tasks

The **cost** includes the salaries of the staff, Employee Benefits (EB), Overhead (OH), and General & Administrative (G&A) rates, which are assumed but are believed to be representative.

The **process** involved estimating the hours required for each staff assigned for each task. Hours were estimated for the non-ACT process that utilizes spreadsheets and documents, and the hours were re-estimated where the team was using the i2ACT-800. The labor required using the i2ACT-800 tool was estimated for the first year and then estimated for subsequent years where the

CAVEAT: It is recognized that the requirements and capabilities of organizations vary greatly. Personnel with significant experience will reduce the number of hours required. Complexity of the network being assessed has a major impact on the cost. The number of staff involved will depend on organization size, network complexity, the number and nature of needed business processes within an organization, and financial constraints. However, the analysis presented is considered representative and therefore, reasonably illustrates the value of employing the i2ACT-800.

benefit of maintaining the information regarding compliance paid even greater savings. The first year and the 5 year Return on Investment (ROI) were calculated.

•CASE STUDY 1: MID-LEVEL BUSINESS / ORGANIZATION

In this case study, the hours required for completion of the tasks both with and without the use of the i2ACT-800 are estimated for the first year or first compliance effort (FIGURE 39). The state of the art for this sort of effort includes using spreadsheets and word documents in a file management system like SharePoint. A good deal of time is required for education and training, the assessment is lengthy and loosely constructed, and a great deal of time is spent caring for the documentation The same information is estimated for the same team using the i2ACT-800 product. These results are shown in FIGURE 40. Dramatic

MID-LEVEL BUSINESS		STAFFING YEAR 1 (BASE)						TOTAL YR1
	TASK	Management &/or Task Lead	Sr. IT Network Engineer	Security Engineer	FSO	HR Trainer	Book Boss / Documentation	TOTALS
1	STANDARDS RESEARCH & EDUCATION	48	40	40	40	20	20	208
2	COMPLIANCE CONTROLS ORGANIZATION	16	16				40	72
3	REQUIREMENTS	4	8	8	4	4	40	68
4	TEAM IDENTIFICATION & ASSEMBLY	6						6
5	TEAM TRAINING	8	16	16	16	16	16	88
6	DATA GATHERING	24	40	40	8	8	80	200
7	COMPLIANCE DOCUMENTATION	16	24	16	16	4	80	156
8	REVIEW & COMPLETE DOCUMENTATION	12	24	24	16	16	40	132
9	AUDIT	8	8	32	16	8	32	104
10	REMEDIATION							0
11	UPDATE DOCUMENTATION	8	8	16	4	2	80	118
	TOTAL HOURS	150	184	192	120	78	428	1152
	SALARY (Annual x 1,000)	$ 100	$ 100	$ 80	$ 80	$ 80	$ 50	
	COST THROUGH EB (30% Benefits)	$ 9,375	$ 11,500	$ 9,600	$ 6,000	$ 3,900	$ 13,375	$ 53,750
	COST THROUGH OH & G&A (50% & 10%)	$ 15,469	$ 18,975	$ 15,840	$ 9,900	$ 6,435	$ 22,069	$ 88,688

FIGURE 39: Manual Cybersecurity Compliance Audit Pro Forma (spreadsheet tool used) Mid-Sized Group

reduction in labor is achieved by reducing the education and training time, and eliminating the staff required for the documentation. The i2ACT-800 also focuses the attention of the staff on the exact requirements for completion eliminating uncertainty. This greatly reduces the staff time required but also improves the quality of the end product.

Assessments should be conducted at least annually and if the i2ACT-800 is maintained throughout the year, the amount of time required for the subsequent years is nearly eliminated (FIGURE 41), and this savings is realized every year thereafter. Making sure that all is up to date for the audit is all that is required.

The savings for the mid-level organization are substantial. In the first year the ratio of savings to cost is over 10:1 and the year 1 ROI is over 900%. The 5-year ROI increases to 1617% with no OH and G&A, and 2774% with the additional loading of labor. Why? The answer is simple. Very expensive labor is replaced or eliminated with an inexpensive software package. It is recognized that every organization will be different and the time required by the staff in different firms will vary greatly. The conclusion regarding value is not sensitive to this variability. Consider this: if the estimates shown are off by a fact of 10 – an

order of magnitude – the ROI would still be positive in the first year or very close to it. It is interesting to note that this is the least attractive return from the three case studies.

MID-LEVEL BUSINESS		STAFFING YEAR 1 (i2ACT)						TOTAL YR1
	TASK	Management &/or Task Lead	Sr. IT Network Engineer	Security Engineer	FSO	HR Trainer	Book Boss / Documentation	TOTALS
1	STANDARDS RESEARCH & EDUCATION	8	8	8	4	4	0	32
2	COMPLIANCE CONTROLS ORGANIZATION						0	0
3	REQUIREMENTS	0	0	0	0	0	0	0
4	TEAM IDENTIFICATION & ASSEMBLY	6						6
5	TEAM TRAINING	4	4	2	2	2	0	14
6	DATA GATHERING	16	32	32	8	8	0	96
7	COMPLIANCE DOCUMENTATION	8	16	16	4	1	0	45
8	REVIEW & COMPLETE DOCUMENTATION	8	8	16	4	4	0	40
9	AUDIT	8	8	32	16	8	0	72
10	REMEDIATION							0
11	UPDATE DOCUMENTATION	4	4	4	2	2	0	16
	TOTAL HOURS	62	80	110	40	29	0	321
	SALARY (Annual x 1,000)	$ 100	$ 100	$ 80	$ 80	$ 80	$ 50	
A	COST THROUGH EB (30% Benefits)	$ 3,875	$ 5,000	$ 5,500	$ 2,000	$ 1,450	$ -	$ 17,825
B	COST THROUGH OH & G&A (50% & 10%)	$ 6,394	$ 8,250	$ 9,075	$ 3,300	$ 2,393	$ -	$ 29,411

FIGURE 40: i2ACT-800 Cybersecurity Compliance Audit Pro Forma (First Year) Mid Group

MID-LEVEL BUSINESS		STAFFING YEAR 1 (i2ACT)						TOTAL YR1
	TASK	Management &/or Task Lead	Sr. IT Network Engineer	Security Engineer	FSO	HR Trainer	Book Boss / Documentation	TOTALS
1	STANDARDS RESEARCH & EDUCATION	8	8	8	4	4	0	32
2	COMPLIANCE CONTROLS ORGANIZATION						0	0
3	REQUIREMENTS	0	0	0	0	0	0	0
4	TEAM IDENTIFICATION & ASSEMBLY	6						6
5	TEAM TRAINING	4	4	2	2	2	0	14
6	DATA GATHERING	16	32	32	8	8	0	96
7	COMPLIANCE DOCUMENTATION	8	16	16	4	1	0	45
8	REVIEW & COMPLETE DOCUMENTATION	8	8	16	4	4	0	40
9	AUDIT	8	8	32	16	8	0	72
10	REMEDIATION							0
11	UPDATE DOCUMENTATION	4	4	4	2	2	0	16
	TOTAL HOURS	62	80	110	40	29	0	321
	SALARY (Annual x 1,000)	$ 100	$ 100	$ 80	$ 80	$ 80	$ 50	
A	COST THROUGH EB (30% Benefits)	$ 3,875	$ 5,000	$ 5,500	$ 2,000	$ 1,450	$ -	$ 17,825
B	COST THROUGH OH & G&A (50% & 10%)	$ 6,394	$ 8,250	$ 9,075	$ 3,300	$ 2,393	$ -	$ 29,411

FIGURE 41: i2ACT-800 Cybersecurity Compliance Audit Pro Forma (Second Year)

•CASE STUDY 2: SMALL BUSINESS

In a small company, a senior staff member will take on the entire job of bringing the firm into compliance, possibly with the assistance of a technical writer or junior staff support. The same analytic procedure was used for this case study. The hours required for the manual assessment and compliance work is shown in FIGURE 42.

SMALL BUSINESS		STAFFING YEAR 1 (BASE)						TOTAL YR1
	TASK	Management &/or Task Lead	Sr. IT Network Engineer	Security Engineer	FSO	HR Trainer	Book Boss / Documentation	TOTALS
1	STANDARDS RESEARCH & EDUCATION			40			20	60
2	COMPLIANCE CONTROLS ORGANIZATION			32			40	72
3	REQUIREMENTS			40			40	80
4	TEAM IDENTIFICATION & ASSEMBLY							0
5	TEAM TRAINING			16			16	32
6	DATA GATHERING			160			80	240
7	COMPLIANCE DOCUMENTATION			80			80	160
8	REVIEW & COMPLETE DOCUMENTATION	12		24			40	76
9	AUDIT			60			32	92
10	REMEDIATION							0
11	UPDATE DOCUMENTATION			32			80	112
	TOTAL HOURS	12	0	484	0	0	428	924
	SALARY (Annual x 1,000)	$ 100	$ 100	$ 80	$ 80	$ 80	$ 50	
	COST THROUGH EB (30% Benefits)	$ 750	$ -	$ 24,200	$ -	$ -	$ 13,375	$ 38,325
	COST THROUGH OH & G&A (50% & 10%)	$ 1,238	$ -	$ 39,930	$ -	$ -	$ 22,069	$ 63,236

FIGURE 42: Small Business Manual Cybersecurity Compliance Audit Pro Forma (Baseline) (Second Year)

The labor required when using the i2ACT-800 is shown in FIGURE 43. There is still significant savings. In fact, the structure and built in aids may well be more important when one or two staff are involved in the compliance effort. This resulted in even higher returns. The first year ROI is over 1800% and the 5-year ROI for the different labor costs are 2703% and 4540%.

•

SMALL BUSINESS		STAFFING YEAR 1 (i2ACT)						TOTAL YR1
	TASK	Management &/or Task Lead	Sr. IT Network Engineer	Security Engineer	FSO	HR Trainer	Book Boss / Documentation	TOTALS
1	STANDARDS RESEARCH & EDUCATION			8			0	8
2	COMPLIANCE CONTROLS ORGANIZATION			0			0	0
3	REQUIREMENTS			0			0	0
4	TEAM IDENTIFICATION & ASSEMBLY							0
5	TEAM TRAINING			4			0	4
6	DATA GATHERING			80			0	80
7	COMPLIANCE DOCUMENTATION			0			0	0
8	REVIEW & COMPLETE DOCUMENTATION	8		8			0	16
9	AUDIT			32			0	32
10	REMEDIATION							0
11	UPDATE DOCUMENTATION			4			0	4
	TOTAL HOURS	8	0	136	0	0	0	144
	SALARY (Annual x 1,000)	$ 100	$ 100	$ 80	$ 80	$ 80	$ 50	
A	COST THROUGH EB (30% Benefits)	$ 500	$ -	$ 6,800	$ -	$ -	$ -	$ 7,300
B	COST THROUGH OH & G&A (50% & 10%)	$ 825	$ -	$ 11,220	$ -	$ -	$ -	$ 12,045

FIGURE 43: i2ACT SmallBusiness Cybersecurity Compliance Audit Pro Forma

•CASE STUDY 3: ENTERPRISE

To illustrate the savings provided to an enterprise organization, the third case study examined an organization that contained both 5 and 10 independent networks. The returns continue to improve. The labor savings is linear with the number of seats and the cost of the software, measured in terms of cost per seat, decreases dramatically as the volume of seats increase.

To illustrate the impact, FIGURE 44 shows the return of the first year for a range of sizes from 1 seat for a small business to 50 seats in a larger enterprise.

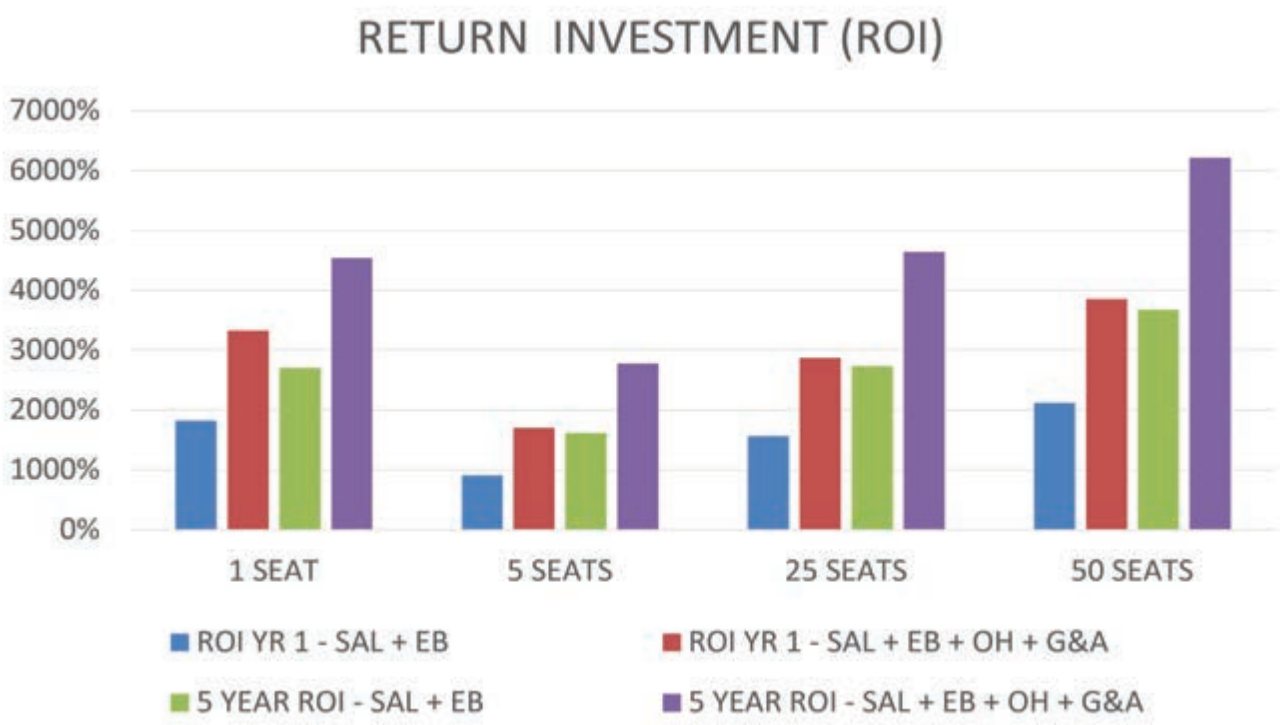

FIGURE 44 Return on Investment Matrix

•CONCLUSIONS

The result of the case studies shows dramatic returns in all cases. The i2ACT-800 tools will reduce the labor required for assessments and compliance efforts. The use of relatively inexpensive software can and will return savings that are many, many times greater than the investment required.

Every organization faces different challenges in their compliance arena and all will have different staff and internal capabilities and resources. Some faster and more capable than others. However, the large leverage provided by the reduction of labor is applicable to all. If the time savings shown in these case studies is off by a factor of 10 - which they are not - the ROI would still be positive in the first year. Combined with increased accuracy, decreased rework and mistakes, make the use of the i2ACT a very positive and decisive decision.

SUMMARY

The i2ACT-800 is a tool that can make implementing the NIST SP 800 series manageable, focusing resources on critical requirements, improving the quality of implementation while increasing the efficiency and decreasing cost. Combining the suite of products such as policies and procedures, cybersecurity plans, incident response plans, disaster recovery plans, and business continuity plans empower the individual companies – even those with limited resources – to be in control of their compliance process. These tools also support ongoing maintenance and continuous improvement for each organization.

Compliance with standards is going to be a pillar of cybersecurity. Organizations need to learn how to effectively apply standards and develop a structure for growth. The NIST SP 800 is a composable structure for determining the appropriate security profile

for organizations large or small across all industries. The RMF provides the guidance for the initial profile and the long-term monitoring and improving of the system. It will grow and be maintained for the long term and is the type of standard that can be relied upon for long term effectiveness. The i2 compliance tools have been specifically designed to provide total support to each organization that needs to comply with the FAR and the DFARS.