



# Automating Authorization using TrustedAgent GRC

This whitepaper discusses the key requirements of the various regulatory and standard frameworks, and addresses how the usage of TrustedAgent GRC can accelerate the implementation and support ongoing compliance activities for the organization.



### The Authorization Process

Security and privacy authorization process requires the organizations to examine their information technology infrastructure and systems, to develop supporting evidence necessary for security and privacy assurance authorization, and a senior official or company management attests to the completion and grants the use of the infrastructure or system. The overall process, while simplistic in definition, can be complex and time-consuming due to the number of activities to be performed. The process also needs resources that strain many organizations by requiring expertise that is both costly and hard to find in today's competitive cybersecurity marketplace. Since the authorization process is continuous in nature requiring ongoing monitoring, update of evidence for changes, and re-testing of controls over time, the organizations incur recurring cost of sustaining the authorization for as long as the IT infrastructure or system is in use.

For the public sector, under one or more regulations, including Federal Information Security Management Act (FISMA), Federal Risk and Authorization Management Program (FedRAMP), and Department of Defense Information Assurance Certification and Accreditation Process (DIACAP), Federal government agencies and organizations that provide IT infrastructure and systems to government agencies must meet the requirements of authorization before their infrastructure or systems can be used. In certain cases, where state and local government agencies receiving Federal grants, the agencies must also comply with the requirements of FISMA.

For the private sector, as the governing regulations and standards become more complex and noncompliance penalties range from multiple hundreds of thousands to millions of dollars, many private organizations across several industries including banking institutions, retailers, health care providers, and others are finding themselves under closer scrutiny from their regulators and industry groups to improve their privacy and security practices. Regulations and standards impacting these organizations include Federal Financial Institutions Examination Council (FFIEC), Payment Card Industry Data Security Standard (PCI DSS), North American Electric Reliability Corporation (NERC)'s Critical Infrastructure Protection (CIP), Health Insurance Portability and Accountability Act (HIPAA), and Health Information Technology for Economic and Clinical Health Act (HITECH). For organizations that have already demonstrated ongoing compliance to these standards/regulations, they seek to elevate their standing with their shareholders and industry peers and reduce their liabilities from incidents and data breaches through voluntary adoption of best practices by leveraging one or more frameworks including NIST Cybersecurity Framework (CSF), COBIT, ISO 27001, or SANS Critical Controls.

### The Automated Solution

By streamlining the key activities of the authorization process, through automation and re-use of common information, standardizations, organizations can comply with the regulations/standards, drive improvements and consistency of practices to business processes for managing compliance activities, and reduce the full-time resources to address initial and sustaining compliance. Over time, organizations can lower exposure to both financial and reputational risks, and improve cost and operating efficiencies. From a good governance and community responsibility perspective, adopters also elevate their standing among their industry-peers, and existing and potential customers, which can bring greater values for the organizations' products and services. Greater adherence to regulatory requirements can also provide or prove regulatory compliance enabling organizations to lower their regulatory and audit risk profile with regulatory bodies and subsequently, lower penalties from noncompliance.

This whitepaper provides the readers with the requirements of the key regulatory and standard frameworks, how they manage authorization process, and addresses how the usage of TrustedAgent GRC can accelerate the implementation and ongoing support of compliance activities for the organization. The whitepaper also offers a financial justification model to support the acquisition through cost savings gained using TrustedAgent GRC by comparing the time savings gained between automation vs. manual methods to implementing key activities.

### Use of Risk Management Approach

No matter which regulations or standards that govern the organizations they all share the common expectation of having adopted a risk management approach that enables organizations to identify risks from various sources in accordance with the defined compliance controls, to analyze and determine the extent of the risks, and to remediate them from further impacting the organizations. Key requirements from one or more regulations or standards citing the usage of risk management framework as part of an organization enterprise risk management include:

Regulations or Standards	Requirements	
COBIT ISO 27001	ISO/IEC 27001-2005 Requirement 4: Establish Information Security Management System (4.1 thru. 4.2.4) A.14.1.2: Business continuity and risk assessment A.14.1.4: Business continuity planning framework	EDM02: Ensure benefits delivery EDM03: Ensure risk optimisation EDM04: Ensure resource optimisation MEA02: Monitor, evaluate and assess the system of internal control
ARS FedRAMP FISMA MARS-E	PM-1: Information Security Program Plan PM-9: Risk Management Strategy	
HIPAA HITECH Meaningful Use	§164.308(a)(1)(ii)(B): Risk Management. Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Sec 164.206(a) → Implement a Risk Management Program.	
NIST CSF	ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders.	
NERC CIP	CIP-007-5: R1 to R5. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in CIP-007-5 Table R1 – Ports and Services, CIP-007-5 Table R2 – Security Patch Management, CIP-007-5 Table R3 – Malicious Code Prevention, CIP-007-5 Table R4 – Security Event Monitoring, and CIP-007-5 Table R5 – System Access Controls.	
PCI DSS	12.2: Implement a risk-assessment process that: <ul style="list-style-type: none"><li>Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.),</li><li>Identifies critical assets, threats, and vulnerabilities, and</li><li>Results in a formal risk assessment.</li></ul> 12.8.4: Maintain a program to monitor service providers’ PCI DSS compliance status at least annually.	
SANS Critical Security Controls	Focuses first on prioritizing security functions that are effective against the latest Advanced Targeted Threats, with a strong emphasis on "What Works" - security controls where products, processes, architectures and services are in use that have demonstrated real world effectiveness. Standardization and automation is another top priority, to gain operational efficiencies while also improving effectiveness.	
<b>Note:</b> → Signifies one or more key activities of the requirement.		

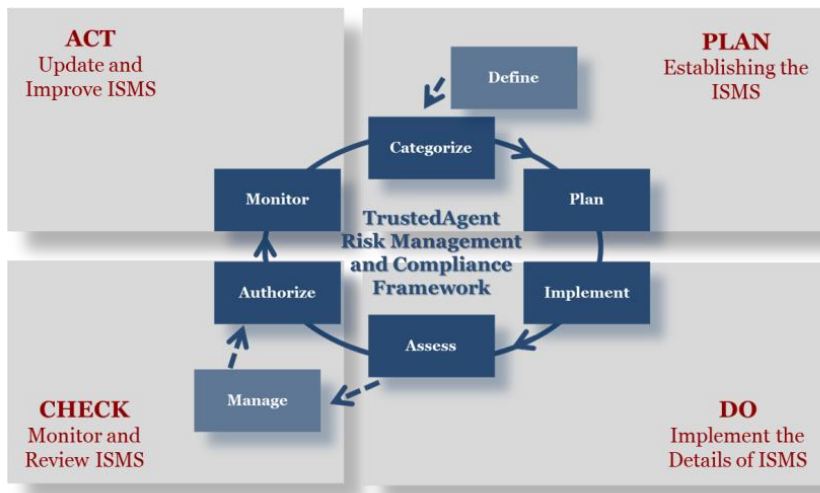
## How TrustedAgent GRC Supports NIST Cybersecurity Framework

TrustedAgent GRC automates IT governance, risk, and compliance processes (GRC) including authorization, compliance, policy management, incident management, vendor and enterprise risk, and vulnerability management in one centrally-managed application. TrustedAgent captures, measures and brings visibility and accountability to business and IT risks across business units, operations, functions, and subsidiaries or vendors. With TrustedAgent, the organization can define entities, business processes, and assets; communicate and track adherence to policies and procedures; conduct risk reviews to particular standard; identify exposed risk areas; manage remediation and mitigation activities; and monitor for ongoing risk and prevent recurrences.



**Figure 1: TrustedAgent Risk Management and Compliance Framework**

TrustedAgent (TA) Risk Management and Compliance Framework (RMCF) is modeled after NIST Risk Management Framework (RMF) (as shown in dark blue) with the exception of the additional step added for defining the organization inventory and the step for managing findings and their associated corrective actions (as shown in light blue). In addition to NIST RMF, TrustedAgent RMCF also maps to ISO 27001, as shown below, and other frameworks including COBIT and NIST Cybersecurity Framework (CSF). Each phase is further described below along with the regulated or standard requirements directly supported.

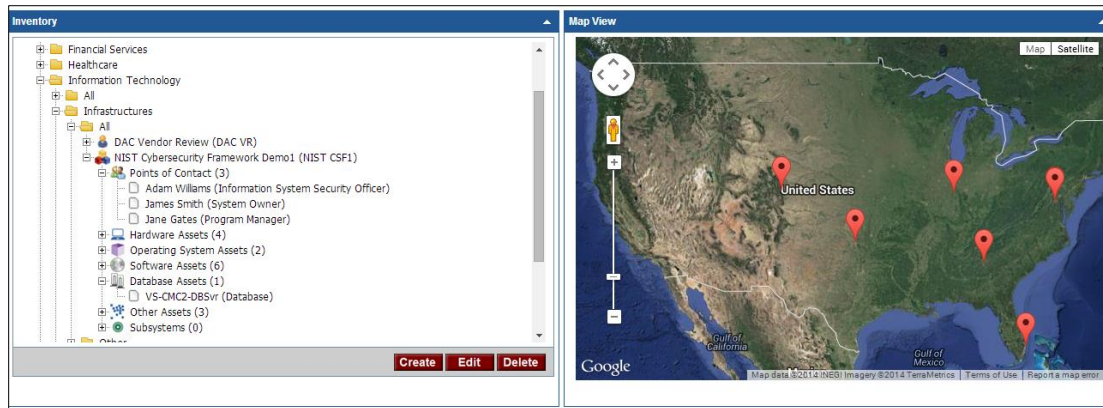


**Figure 2: ISO 27001 vs. TrustedAgent Risk Management and Compliance Framework**

interconnections, etc.) and hardware and software assets and devices supporting the inventory item must be maintained. The list serves as the initial basis from which the organization can conduct the extent their exposure to the various risks across multiple regulations or standards. Highlights of key regulations/standards and the requirements addressable by TrustedAgent for this phase include:

Regulations or Standards	Requirements	
COBIT ISO 27001	A.7.1.1: Inventory of assets A.7.1.2: Ownership of assets A.7.2.1: Classification guidelines A.8.1.1: Roles and responsibilities A.8.2.1: Management responsibilities A.10.8.2: Exchange agreements	APO08: Manage Relationships APO09: Manage Service Agreements BAI04: Manage Availability and Capacity BAI09: Manage Assets BAI10: Manage Configuration
ARS FISMA MARS-E	CM-8: Information System Component Inventory PM-5: Information System Inventory CA-3: System Interconnections CA-9: Internal System Connections	
HIPAA HITECH Meaningful Use	§164.308(a)(1)(i): Security Management Process. Implement policies and procedures to prevent, detect, contain and correct security violations → Identify relevant information systems (that house or process ePHI). §164.308(a)(1)(ii)(B): Risk Management. Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Sec 164.206(a) → Acquire IT systems and services. §164.402: Definitions - Breach means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information. (1)(i) For purposes of this definition, compromises the security or privacy of the protected health information means poses a significant risk of financial, reputational, or other harm to the individual. (ii) A use or disclosure of protected health information that does not include the identifiers listed at §164.514(e)(2), date of birth, and zip code does not compromise the security or privacy of the protected health information. → Risk Assessment of Breach	
NIST CSF	ID.AM-1: Physical devices and systems within the organization are inventoried. ID.AM-2: Software platforms and applications within the organization are inventoried. ID.AM-4: External information systems are catalogued. ID.AM-3: Organizational communication and data flows are mapped. ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on the classification, criticality, and business value. ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established. ID.BE-1: The organization's role in the supply chain and is identified and communicated. ID.BE-2: The organization's place in critical infrastructure and their industry ecosystem is identified and communicated. RS.IP-2: A System Development Life Cycle (SDLC) to manage systems is implemented. DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed. DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability. RS.CO-2: Events are reported consistent with established criteria.	
NERC CIP	CIP-002-5 BES Cyber System Categorization: R1: Attachment 1 CIP-002-5 Incorporates the "Bright Line Criteria" to classify BES Assets as Low, Medium, or High. Called BES Cyber Systems consolidating CAs and CCAs. CIP-002-5 BES Cyber System Categorization: R2: BES Cyber System Lists must be reviewed and approved every 15 calendar months	
PCI DSS	2.4 Maintain an inventory of system components that are in scope for PCI DSS. 11.1.1 Maintain an inventory of authorized wireless access points including a documented business justification.	
SANS Critical Security Controls	CSC-1: Inventory of Authorized and Unauthorized Devices CSC-2: Inventory of Authorized and Unauthorized Software	

TrustedAgent provides a centralized platform allowing the tracking of inventory of entities. Types of entities can be tracked include systems, programs, sites (such as data centers), and vendors. These entities represent the possible inventories or sources of privacy or security concerns or critical infrastructure assets for cyber-attacks. Each entity is further associated with a collection of hardware and software items that represent smaller key components of the entity.



**Figure 3: Inventory of Entities**

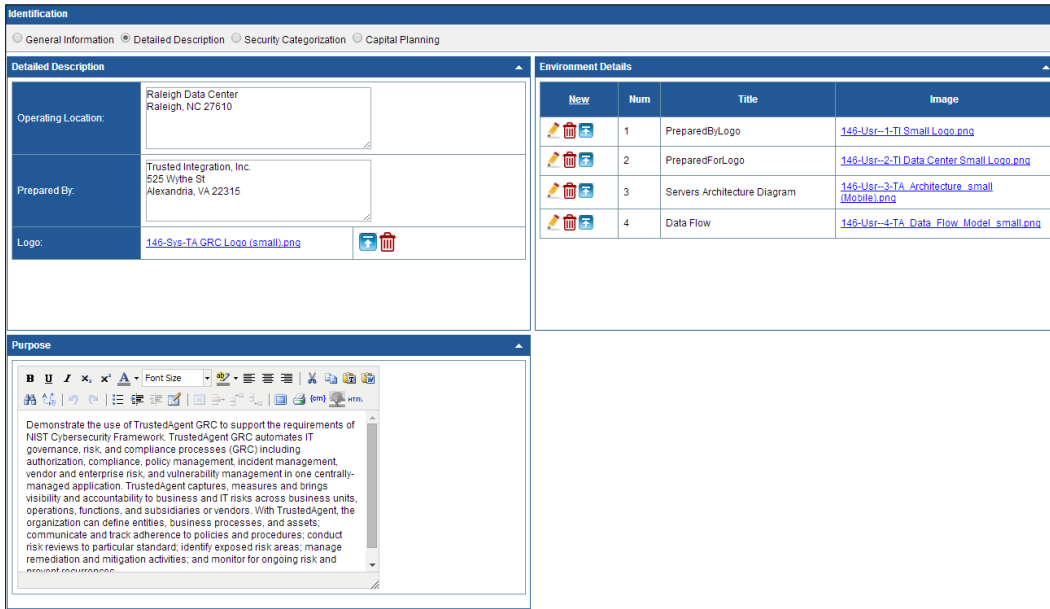
Identification   People and Inventory   Controls   Findings   Authorization   Reports									
Inventory									
Rows per page: 100		View By: User Access POCs Interconnections <b>Inventory</b> Subsystems							
	New	Name	Parent Entity	Parent Asset	Type	Vendor	Product	Version	Hostname(s)
<input type="checkbox"/>		EPHI-AK-ZCA1 - VM	Not Applicable	EPHI-AK-ZCA1	Software	EMC	EMC VMware		
<input type="checkbox"/>		EPHI-AK-ZCA1	Not Applicable	Not Applicable	Hardware	Dell	Dell 3000cn		
<input type="checkbox"/>		EPHI-AK-ZCA2 - VM	Not Applicable	EPHI-AK-ZCA2	Software	EMC	EMC VMware		
<input type="checkbox"/>		EPHI-AK-ZCA2	Not Applicable	Not Applicable	Hardware	Dell	Dell Poweredge 2950		
<input type="checkbox"/>		EPHI-AK-ZCA1 - OS	Not Applicable	EPHI-AK-ZCA1	Operating System	Microsoft	Microsoft Windows Server 2008 x64 (64-bit)	x64	
<input type="checkbox"/>		EPHI-AK-ZCA1 - App Server	Not Applicable	EPHI-AK-ZCA1	Software	Apache	Apache Software Foundation Tomcat		
<input type="checkbox"/>		EPHI-AK-ZCA1 - TrustedAgent	Not Applicable	EPHI-AK-ZCA1	Software	Trusted Integration	TrustedAgent GRC	5.0.3	
<input type="checkbox"/>		EPHI-AK-ZCA2 - OS	Not Applicable	EPHI-AK-ZCA2	Operating System	Microsoft	Microsoft Windows Server 2008 x64 (64-bit)	x64	
<input type="checkbox"/>		EPHI-AK-ZCA2 - DB Server	IT Security Demo Data Center	ITSDOC-KIW-ZCA2 - DB Schema	Database	Microsoft	Microsoft SQL Server 2008 R2 Service Pack 1 X64 (64-bit)	2008	
<input type="checkbox"/>		eeyesolutions.corp.int-eeeye.com	Not Applicable	Not Applicable	Software	Eeye	Eeye Retina 5.10.12.1700	5.10.12.1700	eeyesolutions.corp.int-eeeye.com
<input type="checkbox"/>		EPHI-AK-ZCA1 - FW1	Not Applicable	EPHI-AK-ZCA1	Hardware	Cisco	Cisco PIX Firewall 535		
<input type="checkbox"/>		EPHI-AK-ZCA1 - FW2	Not Applicable	EPHI-AK-ZCA1	Hardware	Cisco	Cisco PIX Firewall 535		
<input type="checkbox"/>		EPHI-AK-ZCA2 - FW1	Not Applicable	EPHI-AK-ZCA2	Hardware	Cisco	Cisco PIX Firewall 535		
<input type="checkbox"/>		EPHI-AK-ZCA2 - FW3	Not Applicable	EPHI-AK-ZCA2	Hardware	Cisco	Cisco PIX Firewall 535		
<input type="checkbox"/>		EPHI-AK-ZCA2 - FW2	Not Applicable	EPHI-AK-ZCA2	Hardware	Cisco	Cisco PIX Firewall 535		
<input type="checkbox"/>		EPHI-AK-ZCA1 - RT1	Not Applicable	EPHI-AK-ZCA1	Hardware	Netgear	Netgear WGR614v8	v8	
<input type="checkbox"/>		EPHI-AK-ZCA2 - RT1	Not Applicable	EPHI-AK-ZCA1	Hardware	Netgear	Netgear WGR614v9	v9	
<input type="checkbox"/>		Test Demo ITEM	Not Applicable	Not Applicable	Software	Omega Suite	Ovi 232		

**Figure 4: Asset and Device Inventory**

TrustedAgent utilizes a common descriptive framework to describe the entities and the relationship to the organization's mission and objectives for directors, management, and organizational staff. Other descriptive attributes include ownership based on organization's hierarchy, general and detail characteristics, points of contact, etc. Information and inventories may be bulk-loaded and be re-used across several reports. Entities are supported throughout their SDLC life cycle, and the entity's SDLC status can be leveraged to filter reports and dashboard views.



Resources can be assigned to the entities that they support within TrustedAgent. Entities can be organized as major application, general support systems, subsystems, minor application, vendor, program, cloud affiliated, data center, etc. Each entity can also be classified as a critical asset, or financial or privacy sensitivity to highlight business value to the organization. For assets (e.g., hardware, software, devices), an aggregated risk score of vulnerabilities using industry vulnerability standards (e.g., CWSS and CVSS) associated with an asset can be leveraged to prioritize remediation efforts.



**Identification**

General Information • Detailed Description • Security Categorization • Capital Planning

**Detailed Description**

Operating Location: Raleigh Data Center  
Raleigh, NC 27610

Prepared By: Trusted Integration, Inc.  
525 Wythe St  
Alexandria, VA 22315

Logo: 146-Sys-TA GRC Logo (small).png

**Environment Details**

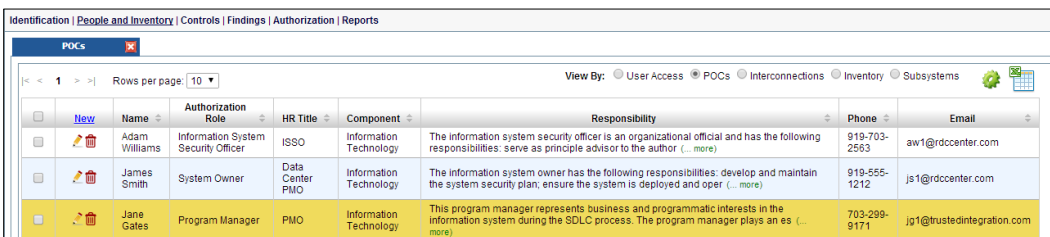
New	Num	Title	Image
	1	PreparedByLogo	146-User-1-TI Small Logo.png
	2	PreparedForLogo	146-User-2-TI Data Center Small Logo.png
	3	Servers Architecture Diagram	146-User-3-TA Architecture_small (Mobile).png
	4	Data Flow	146-User-4-TA Data Flow Model_small.png

**Purpose**

Demonstrate the use of TrustedAgent GRC to support the requirements of NIST Cybersecurity Framework. TrustedAgent GRC automates IT governance, risk, and compliance processes (GRC) including authorization, compliance, policy management, incident management, vendor and enterprise risk, and vulnerability management in one centrally-managed application. TrustedAgent captures, measures and brings visibility and accountability to business and IT risks across business units, operations, functions, and subsidiaries or vendors. With TrustedAgent, the organization can define entities, business processes, and assets; communicate and track adherence to policies and procedures; conduct risk reviews to particular standard; identify exposed risk areas; manage remediation and mitigation activities; and monitor for ongoing risk and associated information.

**Figure 5: Repository of Reusable Key Diagrams**

TrustedAgent enables entities to maintain key personnel and monitoring strategy as part of their continuous monitoring effort. Key contacts may also be applied to incidents reporting, findings, and corrective actions for incidents, BCP and other regulatory activities simplifying staff management, enforcing consistency, and reducing overall errors. Dashboard ensures visibility and accountability to address risks across the organization. Access to information maintained within TrustedAgent is role-based. Several levels of access are available ranging from a complete access using an organization-wide oversight role, to business unit users where limited access to entities within specific business operation/function, and as narrow as specific entity-access such as an information system security officer.



Identification | **People and Inventory** | Controls | Findings | Authorization | Reports

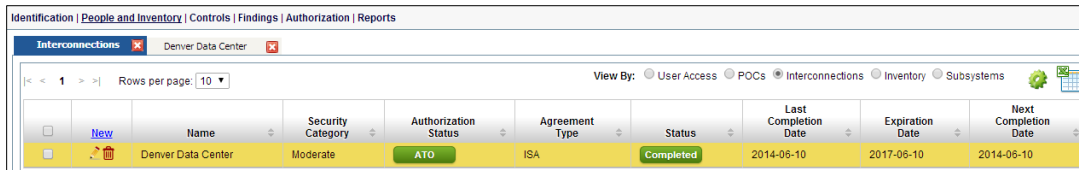
POCs


View By: User Access • POCs • Interconnections • Inventory • Subsystems

	New	Name	Authorization Role	HR Title	Component	Responsibility	Phone	Email
		Adam Williams	Information System Security Officer	ISSO	Information Technology	The information system security officer is an organizational official and has the following responsibilities: serve as principle advisor to the author (... more)	919-703-2563	aw1@rdcenter.com
		James Smith	System Owner	Data Center PMO	Information Technology	The information system owner has the following responsibilities: develop and maintain the system security plan; ensure the system is deployed and oper (... more)	919-555-1212	js1@rdcenter.com
		Jane Gales	Program Manager	PMO	Information Technology	This program manager represents business and programmatic interests in the information system during the SDLC process. The program manager plays an es (... more)	703-299-9171	jp1@trustedintegration.com

**Figure 6: Key Contacts**

Managing interconnections play a significant role in reducing the risks impacting supply chain or critical services from leveraging infrastructures, services, or solutions offered by third-parties, business associates, or vendors. TrustedAgent enables interconnections between information systems within the organization and to external entities outside of the organization to be managed along with characteristics of the information exchange, security and service level agreements, key contacts, and the authorization.



Identification   People and Inventory   Controls   Findings   Authorization   Reports									
Interconnections Denver Data Center									
View By: <input type="radio"/> User Access <input type="radio"/> POCs <input checked="" type="radio"/> Interconnections <input type="radio"/> Inventory <input type="radio"/> Subsystems									
	Name	Security Category	Authorization Status	Agreement Type	Status	Last Completion Date	Expiration Date	Next Completion Date	
	Denver Data Center	Moderate	ATO	ISA	Completed	2014-05-10	2017-06-10	2014-06-10	

**Figure 7: Interconnections**

The central management of policies and procedures is another key capability desired by organizations to support their compliance to one or more regulations and standards.

Regulations or Standards	Requirements	
COBIT ISO 27001	APO01: Manage the IT Management Framework BAI06: Manage Changes A.5.1.1: Information security policy document A.5.1.2: Review of the information security policy A.6.1.2: Information security coordination A.6.1.3: Allocation of information security responsibilities A.8.2.2: Information security awareness, education and training	A.10.1.1: Documented operating procedures A.10.7.3: Information handling procedures A.10.8.1: Information exchange policies and procedures A.11.1.1: Access control policy A.12.5.1: Change control procedures A.13.2.1: Incident responsibilities and procedures
ARS FedRAMP FISMA MARS-E	XX-1: Policies and Procedures (where XX may represent AC-1,AT-1,AU-1,CA-1,CM-1,CP-1,IA-1,IR-1,MA-1,MP-1,PE-1,PL-1,PM-13,PS-1,RA-1,SA-1,SC-1,SI-1 for specific control families)	
HIPAA HITECH Meaningful Use	§164.308(a)(6)(i): Security Incident Procedures. Implement policies and procedures to address security incidents.	
NIST CSF	ID.GV-1: Organizational information security policy is established. ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners.	
NERC CIP	CIP-003-5: Cyber Security - Security Management Controls (R1, R2)	
PCI DSS	12.1: Establish, publish, maintain, and disseminate a security policy.	
SANS Critical security Controls	CSC-9: Security Skills Assessment and Appropriate Training to Fill Gaps	

For the requirements above, TrustedAgent provides a repository of standard policies and procedures that users can leverage and customize for their organizations. Optionally, organizations can develop and publish existing policies and procedures, and distribute them to organization-wide users. Policies and procedures can also be incorporated into organization-specific control requirements based on governing regulations or standards. User roles and responsibilities can be associated with established policies and procedures in TrustedAgent, and be published to users to track adherence of the policies/procedures and by users.



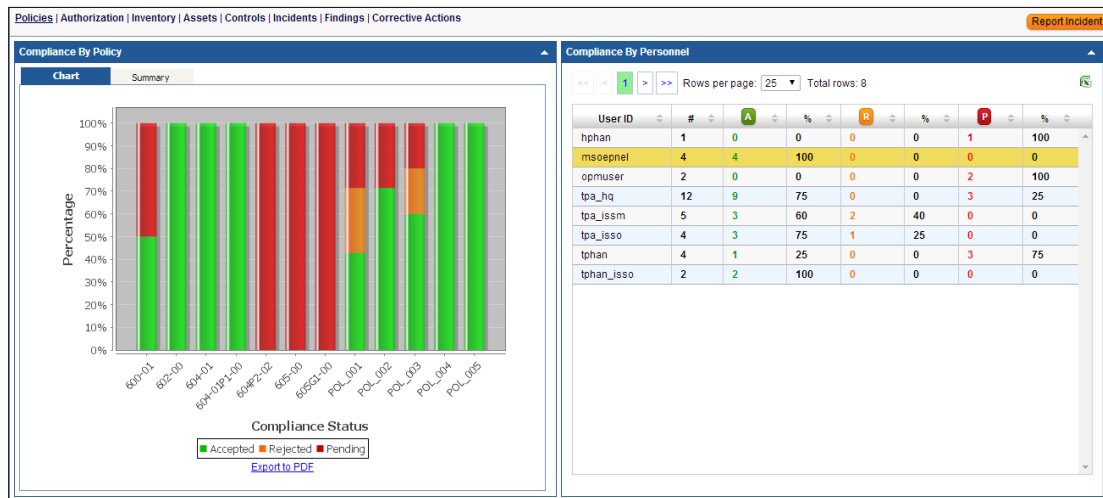


Figure 8: Policy Management

## 2 CATEGORIZE Phase

Security categorization processes are employed to determine applicable security requirements and to establish the baseline risk rating and baseline controls for an entity according to the governing regulation or standard selected. Categorization is based on a specific control template established when the entity is first created. Once established, baseline controls can be tailored across the various components and business units within the organization.

Regulations or Standards	Requirements	
COBIT ISO 27001	DSS01: Manage operations. DSS04: Manage continuity. DSS05: Manage security services.	DSS06: Manage business process controls. A.7.2.1: Classification guidelines A.14.1.2: Business continuity and risk assessment
ARS FedRAMP FISMA MARS-E	RA-2: Security Categorization	
HIPAA HITECH Meaningful Use	<p>§164.308(a)(1)(i): Security Management Process. Implement policies and procedures to prevent, detect, contain and correct security violations. → Have the types of information and uses of that information been identified and the sensitivity of each type of information been evaluated? (See FIPS 199 and SP 800-60 for more on categorization of sensitivity levels.)</p> <p>§164.308(a)(8): Evaluation. Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that established the extent to which an entity's security policies and procedures meet the requirements of this subpart. → Determine Whether Internal or External Evaluation Is Most Appropriate. Develop Standards and Measurements for Reviewing All Standards and Implementation Specifications of the Security Rule.</p>	
NIST CSF	ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated.	
NERC CIP	CIP-002-5: BES Cyber System Categorization: R1: Attachment 1 CIP-002-5 Incorporates the "Bright Line Criteria" to classify BES Assets as Low, Medium, or High. Called BES Cyber Systems consolidating CAs and CCAs.	
PCI DSS	<i>Recommended as best practices.</i>	
SANS Critical Security Controls	CSC-15: Controlled Access Based on the Need to Know	

Organizations can prioritize (or categorize) entities to determine the risk rating using standard methods including NIST 800-60 (using information types managed), FIPS (using confidentiality, integrity, or availability), or maturity level (based on Cybersecurity maturity tiers). The resulting risk rating from the categorization subsequently determines the control requirements according to the selected regulatory or industry standards. TrustedAgent automates security categorization process using NIST 800-60 or by usage of Personally Identifiable Information (PII), thereby significantly reduces the effort to establish control baseline for implementation and assessment.

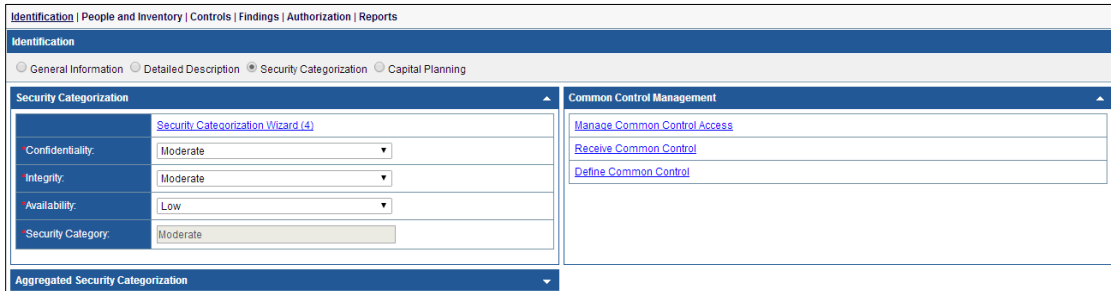


Figure 9: Security Categorization



New	Information Category	Information Type	Name	Justification	Confidentiality	Integrity	Availability	Default Confidentiality	Default Integrity	Default Availability
	C.2.1 Controls and Oversight	C.2.1.1 Corrective Action	C.2.1.1 Controls and Oversight: Corrective Action		Low	Low	Low	Low	Low	Low
	C.3.5 Information and Technology Management	C.3.5.3 System Maintenance	C.3.5.3 Information and Technology Management: System Maintenance		Low	Moderate	Low	Low	Moderate	Low
	C.3.5 Information and Technology Management	C.3.5.5 Information System Security	C.3.5.5 Information and Technology Management: Information System Security		Low	Moderate	Low	Low	Moderate	Low
	C.3.5 Information and Technology Management	C.3.5.8 System and Network Monitoring	C.3.5.8 Information and Technology Management: System and Network Monitoring		Moderate	Moderate	Low	Moderate	Moderate	Low

Figure 10: Categorization Wizard

### 3 PLAN Phase

Critical entities and relationship to other entities can be defined using a parent/child or program or site relationship. Common controls can be established to promote critical functions and services provided across the organization. Controls can also be scoped or tailored to the appropriate level representative of the critical functions or services. Controls can be distributed to one or more TrustedAgent end-users for control implementation to be consistent to their roles and responsibilities. Control Assessment Plan and Security Requirements Traceability Matrix (SRTM) can also be generated by TrustedAgent.

Regulations or Standards	Requirements	
COBIT ISO 27001	A.6.2.2: Addressing security when dealing with customers A.6.2.3: Addressing security in third party agreements	A.10.2.1: Service delivery DSS05: Manage security services.
ARS FEDRAMP FISMA MARS-E	CA-7: Continuous Monitoring CM-2: Baseline Configuration PL-9: Central Management PM-1: Information Security Program Plan	

Regulations or Standards	Requirements
HIPAA HITECH Meaningful Use	§164.308(a)(8): Evaluation. Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that established the extent to which an entity's security policies and procedures meet the requirements of this subpart. → Determine Whether Internal or External Evaluation Is Most Appropriate. Develop Standards and Measurements for Reviewing All Standards and Implementation Specifications of the Security Rule.
NIST CSF	ID.BE-4: Dependencies and critical functions for delivery of critical services are established.
NERC CIP	CIP-003: Security Management Controls
PCI DSS	1.1.2: Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks 1.1.3: Current diagram that shows all cardholder data flows across systems and networks
SANS Critical Security Controls	<i>Recommended as best practices.</i>

Receive Common Control				
Family	Control Title	Maps to Control	Raleigh Data Center	
Access Control			<input checked="" type="radio"/> Inherited	<input type="radio"/> None
Anomalies and Events			<input type="radio"/> Inherited	<input checked="" type="radio"/> None
Asset Management			<input type="radio"/> Inherited	<input checked="" type="radio"/> None
Awareness and Training			<input type="radio"/> Inherited	<input checked="" type="radio"/> None
Business Environment			<input type="radio"/> Inherited	<input checked="" type="radio"/> None
Data Security			<input checked="" type="radio"/> Inherited	<input type="radio"/> None
Detection Processes			<input type="radio"/> Inherited	<input checked="" type="radio"/> None
Governance			<input type="radio"/> Inherited	<input checked="" type="radio"/> None
Information Protection Processes and Procedures			<input checked="" type="radio"/> Inherited	<input type="radio"/> None
Maintenance			<input checked="" type="radio"/> Inherited	<input type="radio"/> None
Protective Technology			<input type="radio"/> Inherited	<input checked="" type="radio"/> None
Recovery Communications			<input type="radio"/> Inherited	<input checked="" type="radio"/> None
Recovery Improvements			<input type="radio"/> Inherited	<input checked="" type="radio"/> None
Recovery Planning			<input type="radio"/> Inherited	<input checked="" type="radio"/> None
Response Analysis			<input type="radio"/> Inherited	<input checked="" type="radio"/> None
Response Communications			<input type="radio"/> Inherited	<input checked="" type="radio"/> None
Response Improvements			<input type="radio"/> Inherited	<input checked="" type="radio"/> None
Response Mitigation			<input type="radio"/> Inherited	<input checked="" type="radio"/> None
Response Planning			<input type="radio"/> Inherited	<input checked="" type="radio"/> None
Risk Assessment			<input type="radio"/> Inherited	<input checked="" type="radio"/> None
Risk Management Strategy			<input type="radio"/> Inherited	<input checked="" type="radio"/> None
Security Continuous Monitoring			<input type="radio"/> Inherited	<input checked="" type="radio"/> None

Figure 11: Receive Common Controls

Identification   People and Inventory   <b>Controls</b>   Findings   Authorization   Reports					
Controls					
<a href="#">Utilities</a> >> Control Scoping					
Control Scoping					
Control:	PR.PT-1				
Confidentiality:	Low				
Integrity:	Moderate				
Availability:	Low				
Security Category:	Moderate				
Justification:	<div></div>				
<input type="button" value="Save"/> <input type="button" value="Close"/>					
Scoping History					
User ID	Justification	Confidentiality	Integrity	Availability	Date
tpa_hq	Control is scope to lower level of confidentiality as no PII is stored.	Low	Moderate	Low	06/11/2014

Figure 12: Control Scoping

Assignment Details

Assign Tasks

User ID:

tpa\_isso

Check All | None

☒ Implementation
 ☐ Annual Assessment
 ☐ ISSM Validation
 ☐ HQ Review

Family / Control	Assign Task	Assigned User	Scheduled Completion Date
ID AM-1 Device and System Inventory	<input checked="" type="checkbox"/>	tpa_isso	12/11/2014
ID AM-2 Software Platform and Application Inventory	<input checked="" type="checkbox"/>	tpa_isso	12/11/2014
ID AM-3 Organizational Interconnections and Data Flows	<input checked="" type="checkbox"/>	tpa_isso	12/11/2014
ID AM-4 External Information System Services	<input checked="" type="checkbox"/>	tpa_isso	12/11/2014
ID AM-5 Prioritization of Resources	<input checked="" type="checkbox"/>	tpa_isso	12/11/2014
ID AM-6 Roles and Responsibilities of Workforce and Third-Party Stakeholders	<input checked="" type="checkbox"/>	tpa_isso	12/11/2014
ID BE-1 Role of Organization and Supply Chain Protection	<input type="checkbox"/>	tpa_isso	
ID BE-2 Critical Infrastructure Plan	<input type="checkbox"/>	tpa_isso	
ID BE-3 Organizational Mission and Business Process Objectives	<input type="checkbox"/>	tpa_isso	
ID BE-4 Dependencies and Functions for Delivery of Critical Services	<input type="checkbox"/>	tpa_isso	
ID BE-5 Resilience and Delivery of Critical Services	<input type="checkbox"/>	tpa_isso	
ID GV-1 Security Policy and Procedures	<input checked="" type="checkbox"/>	tpa_isso	12/11/2014
ID GV-2 Information Security Roles and Responsibilities	<input checked="" type="checkbox"/>	tpa_isso	12/11/2014
ID GV-3 Cybersecurity Legal and Regulatory Requirements	<input checked="" type="checkbox"/>	tpa_isso	12/11/2014

Figure 13: Control Assignment

#### 4 IMPLEMENT Phase

The controls are implemented and documented accordance with organizational, regulatory and standard requirements. System security plans or other organizational documents can be generated to report on control implementation status and compliance details. TrustedAgent offers a large collection of open-source and commercial regulatory and industry standards to accelerate and maintain cybersecurity, regulatory or industry compliance program.

Regulations or Standards	Requirements	
COBIT ISO 27001	A.15.1: Compliance with legal requirements - To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements (A.15.1.1 through A.15.1.6). A.15.2: Compliance with security policies and standards, and technical compliance - To ensure compliance of systems with organizational security policies and standards (A.15.2.1 through A.15.2.2).	MEA01: Monitor, Evaluate and Assess Performance and Conformance MEA02: Monitor, Evaluate and Assess the System of Internal Control MEA03: Monitor, Evaluate and Assess Compliance with External Requirements
ARS FEDRAMP FISMA MARS-E	CA-2: Security Assessments CA-7: Continuous Monitoring	

Regulations or Standards	Requirements
HIPAA HITECH Meaningful Use	<p>§164.308(a)(8): Evaluation. Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that established the extent to which an entity's security policies and procedures meet the requirements of this subpart. → Conduct Evaluation.</p> <p>§164.312(b): Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. → Implement the Audit/System Activity Review Process.</p> <p>Meaningful Use Core Objective &amp; Measure #15: Protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities. → Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process.</p>
NIST CSF	<p>ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.</p> <p>ID.GV-4: Governance and risk management processes address cybersecurity risks.</p> <p>ID.RM-2: Organizational risk tolerance is determined and clearly expressed</p> <p>ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis</p>
NERC CIP	CIP-003: Security Management Controls
PCI DSS	<p><i>Best Practices - Business-as-Usual Processes.</i> Review changes to the environment (for example, addition of new systems, changes in system or network configurations) prior to completion of the change, and perform the following:</p> <ul style="list-style-type: none"> <li>• Determine the potential impact to PCI DSS scope (for example, a new firewall rule that permits connectivity between a system in the CDE and another system could bring additional systems or networks into scope for PCI DSS).</li> <li>• Identify PCI DSS requirements applicable to systems and networks affected by the changes (for example, if a new system is in scope for PCI DSS, it would need to be configured per system configuration standards, including FIM, AV, patches, audit logging, etc., and would need to be added to the quarterly vulnerability scan schedule).</li> <li>• Update PCI DSS scope and implement security controls as appropriate.</li> </ul>
SANS Critical Security Controls	<i>Recommended as best practices.</i>

System owners can document the implementation of their compliance controls established from security categorization. Artifacts supporting compliance can be uploaded and centrally managed to support compliance. TrustedAgent also supports use of compensating controls where primary control implementation may not be adequate to support the requirements. TrustedAgent also enables organization-specific policies or procedures centrally managed using the policy management module to be incorporated into control requirements to help organization personnel with the control implementation.

Controls can also be subset, assigned and distributed to multiple personnel for implementation without needing access to TrustedAgent application using an Excel workbook. The resulting controls can subsequently be imported back into TrustedAgent, therefore significantly enhances portability and efficiency of the workforce resource. Accountability and visibility are improved as control implementation and user performance are also visible on the dashboard.

Identification | People and Inventory | Controls | Findings | Authorization | Reports

Control Implementation

Implementation Assessment Utilities

Search For:  Go

First Previous Next Last (View All)

**General Description**

Class / Family: Identify Asset Management

Control Title: IDAM-1 Device and System Inventory

Description: IDAM-1 Device and System Inventory

Control: Physical devices and systems within the organization are inventoried

**Detailed Description**

Related Controls:

- CCS CSC 1
- COBIT 5 BA09.01, BA09.02
- ISA 62443-2-1:2009 4.2.3.4
- ISA 62443-3-3:2013 SR 7.8
- ISO/IEC 27001:2013 8.8.1.1, 8.8.1.2
- NIST SP 800-53 Rev. 4 CM-8

Supplemental Guidance:

**IDAM-1 Device and System Inventory**

Guidance: Asset Management (IDAM). The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.

**Compliance Information**

Risk Level: Moderate

CIS: ☒ In Place ☐ Partially In Place ☐ Planned ☐ Not Started ☐ Risk Based Decision ☐ User N/A ☐ Hybrid

SCE: ☐ Fully Satisfied ☐ Partially Satisfied ☒ Not Satisfied ☐ Not Applicable

Compliance Description:

The organization utilizes TrustedAgent GRC to support the management of its device and system inventory. TrustedAgent provides a centralized platform allowing the tracking of inventory of entities. Types of entities include systems, programs, sites (such as data centers), and vendors. These entities represent the key inventories or sources for cyber-attacks.

Each entity is further associated with a collection of hardware and software items that represent smaller key components of the entity. The risk profile of an entity tends to increase with increasing number of items in the collection.

**Filters**

CIS: ☒ In Place ☐ Partially In Place ☐ Planned ☐ Not Started ☐ Risk Based Decision ☐ User N/A ☐ None Selected

SCE: ☒ Fully Satisfied ☐ Partially Satisfied ☐ Not Satisfied ☐ Not Applicable

User: All

Type: All

Risk: All

**Common Controls**

☐ Include ☐ Include Only ☐ Exclude

**Hybrid**

☐ Include ☐ Include Only ☐ Exclude

**Continuous Monitoring**

**Assessment**

☐ Include ☐ Include Only ☐ Exclude

**Component**

☐ Include ☐ Include Only ☐ Exclude

**HQ**

☐ Include ☐ Include Only ☐ Exclude

**Controls (110) (M)**

**Asset Management (6) (M)**

- IDAM-1 Device and System Inventory (IP) (M)
- IDAM-2 Software Platform and Application Inventory (IP) (M)
- IDAM-3 Organizational Interconnections and Data Flows (IP) (M)
- IDAM-4 External Information System Services (IP) (M)
- IDAM-5 Prioritization of Resources (IP) (M)
- IDAM-6 Roles and Responsibilities of Workforce and Third-Party Stakeholders (IP) (M)

**Governance (4) (M)**

- Risk Assessment (6) (M)
- Risk Management Strategy (3) (M)
- Access Control (5) (M)
- Awareness and Training (5) (M)
- Data Security (7) (M)
- Information Protection Processes and Procedures (12) (M)

Figure 14: Control Implementation

System security plans or similar documents are automated for end-users based on organizational templates to demonstrate control implementation. TrustedAgent's template authoring also allows the organization to define or revise controls associated with the selected framework with organization-specific requirements, response/implementation standards, and best practices.

System Security Plan (SP) Review Demo

May 14, 2014

Version: 1.0

**EPHI Review Demo1 (cPHI-Demo1)**

**TrustedAgent**  
GOVERNANCE, RISK AND COMPLIANCE

**System Security Plan**  
**EPHI Review Demo1**

Version: 1.0

May 14, 2014

**PROPRIETARY AND CONFIDENTIAL**

Page 1

System Security Plan (SP) Review Demo

May 14, 2014

Version: 1.0

**9.0 General System Description**

This section describes the implementation of administrative actions, and policies and procedures, to manage the collection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of such information.

**9.1 System Function or Purpose**

This section includes a general description of the EPHI Review Demo1. The overall assessment process on leverage uses many risk management frameworks. A detailed example of how the control can be implemented and assessed is provided in the IDAM-1 Device and System Inventory.

For example, in this example, NIST Risk Management Framework is utilized.

The data flow for model within TrustedAgent is as follows:

**Information Flow Diagram**

TrustedAgent supports a variety of methods for data capture including:

- Risk based forecasting capabilities (implication value matrix) including bold, italicized, large font, subscript, superscript, color, underline, etc.
- drag/drop of artifacts/images
- forecasted data capture from fully customizable by the organization
- use of checkboxes, tables, and complex forecasting within tables

**14.0 Administrative Safeguards**

This section describes the implementation of administrative actions, and policies and procedures, to manage the collection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of such information.

**14.1 Security Management Process (SMP)**

**14.1.1 SMP 164.160(a)(1)(i) Security Management Process**

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: Internal

Control Owner: Information Security

Control Description: This control is implemented through the organization's security policies and procedures.

**14.1.2 SMP 164.160(a)(1)(ii) Security Management Process**

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: Internal

Control Owner: Information Security

Control Description: This control is implemented through the organization's security policies and procedures.

**Table 2-1: Sensitivity Categorization of Information Types**

Name	Information Category	Classification	Integrity	Availability	Confidentiality
1.1.1.1 Health Care Information	Health Care Information	High	High	High	High
1.1.1.2 Health Care Information	Health Care Information	High	High	High	High
1.1.1.3 Health Care Information	Health Care Information	High	High	High	High
1.1.1.4 Health Care Information	Health Care Information	High	High	High	High
1.1.1.5 Health Care Information	Health Care Information	High	High	High	High
1.1.1.6 Health Care Information	Health Care Information	High	High	High	High
1.1.1.7 Health Care Information	Health Care Information	High	High	High	High
1.1.1.8 Health Care Information	Health Care Information	High	High	High	High
1.1.1.9 Health Care Information	Health Care Information	High	High	High	High
1.1.1.10 Health Care Information	Health Care Information	High	High	High	High
1.1.1.11 Health Care Information	Health Care Information	High	High	High	High
1.1.1.12 Health Care Information	Health Care Information	High	High	High	High
1.1.1.13 Health Care Information	Health Care Information	High	High	High	High
1.1.1.14 Health Care Information	Health Care Information	High	High	High	High
1.1.1.15 Health Care Information	Health Care Information	High	High	High	High
1.1.1.16 Health Care Information	Health Care Information	High	High	High	High
1.1.1.17 Health Care Information	Health Care Information	High	High	High	High
1.1.1.18 Health Care Information	Health Care Information	High	High	High	High
1.1.1.19 Health Care Information	Health Care Information	High	High	High	High
1.1.1.20 Health Care Information	Health Care Information	High	High	High	High
1.1.1.21 Health Care Information	Health Care Information	High	High	High	High
1.1.1.22 Health Care Information	Health Care Information	High	High	High	High
1.1.1.23 Health Care Information	Health Care Information	High	High	High	High
1.1.1.24 Health Care Information	Health Care Information	High	High	High	High
1.1.1.25 Health Care Information	Health Care Information	High	High	High	High
1.1.1.26 Health Care Information	Health Care Information	High	High	High	High
1.1.1.27 Health Care Information	Health Care Information	High	High	High	High
1.1.1.28 Health Care Information	Health Care Information	High	High	High	High
1.1.1.29 Health Care Information	Health Care Information	High	High	High	High
1.1.1.30 Health Care Information	Health Care Information	High	High	High	High
1.1.1.31 Health Care Information	Health Care Information	High	High	High	High
1.1.1.32 Health Care Information	Health Care Information	High	High	High	High
1.1.1.33 Health Care Information	Health Care Information	High	High	High	High
1.1.1.34 Health Care Information	Health Care Information	High	High	High	High
1.1.1.35 Health Care Information	Health Care Information	High	High	High	High
1.1.1.36 Health Care Information	Health Care Information	High	High	High	High
1.1.1.37 Health Care Information	Health Care Information	High	High	High	High
1.1.1.38 Health Care Information	Health Care Information	High	High	High	High
1.1.1.39 Health Care Information	Health Care Information	High	High	High	High
1.1.1.40 Health Care Information	Health Care Information	High	High	High	High
1.1.1.41 Health Care Information	Health Care Information	High	High	High	High
1.1.1.42 Health Care Information	Health Care Information	High	High	High	High
1.1.1.43 Health Care Information	Health Care Information	High	High	High	High
1.1.1.44 Health Care Information	Health Care Information	High	High	High	High
1.1.1.45 Health Care Information	Health Care Information	High	High	High	High
1.1.1.46 Health Care Information	Health Care Information	High	High	High	High
1.1.1.47 Health Care Information	Health Care Information	High	High	High	High
1.1.1.48 Health Care Information	Health Care Information	High	High	High	High
1.1.1.49 Health Care Information	Health Care Information	High	High	High	High
1.1.1.50 Health Care Information	Health Care Information	High	High	High	High
1.1.1.51 Health Care Information	Health Care Information	High	High	High	High
1.1.1.52 Health Care Information	Health Care Information	High	High	High	High
1.1.1.53 Health Care Information	Health Care Information	High	High	High	High
1.1.1.54 Health Care Information	Health Care Information	High	High	High	High
1.1.1.55 Health Care Information	Health Care Information	High	High	High	High
1.1.1.56 Health Care Information	Health Care Information	High	High	High	High
1.1.1.57 Health Care Information	Health Care Information	High	High	High	High
1.1.1.58 Health Care Information	Health Care Information	High	High	High	High
1.1.1.59 Health Care Information	Health Care Information	High	High	High	High
1.1.1.60 Health Care Information	Health Care Information	High	High	High	High
1.1.1.61 Health Care Information	Health Care Information	High	High	High	High
1.1.1.62 Health Care Information	Health Care Information	High	High	High	High
1.1.1.63 Health Care Information	Health Care Information	High	High	High	High
1.1.1.64 Health Care Information	Health Care Information	High	High	High	High
1.1.1.65 Health Care Information	Health Care Information	High	High	High	High
1.1.1.66 Health Care Information	Health Care Information	High	High	High	High
1.1.1.67 Health Care Information	Health Care Information	High	High	High	High
1.1.1.68 Health Care Information	Health Care Information	High	High	High	High
1.1.1.69 Health Care Information	Health Care Information	High	High	High	High
1.1.1.70 Health Care Information	Health Care Information	High	High	High	High
1.1.1.71 Health Care Information	Health Care Information	High	High	High	High
1.1.1.72 Health Care Information	Health Care Information	High	High	High	High
1.1.1.73 Health Care Information	Health Care Information	High	High	High	High
1.1.1.74 Health Care Information	Health Care Information	High	High	High	High
1.1.1.75 Health Care Information	Health Care Information	High	High	High	High
1.1.1.76 Health Care Information	Health Care Information	High	High	High	High
1.1.1.77 Health Care Information	Health Care Information	High	High	High	High
1.1.1.78 Health Care Information	Health Care Information	High	High	High	High
1.1.1.79 Health Care Information	Health Care Information	High	High	High	High
1.1.1.80 Health Care Information	Health Care Information	High	High	High	High
1.1.1.81 Health Care Information	Health Care Information	High	High	High	High
1.1.1.82 Health Care Information	Health Care Information	High	High	High	High
1.1.1.83 Health Care Information	Health Care Information	High	High	High	High
1.1.1.84 Health Care Information	Health Care Information	High	High	High	High
1.1.1.85 Health Care Information	Health Care Information	High	High	High	High
1.1.1.86 Health Care Information	Health Care Information	High	High	High	High
1.1.1.87 Health Care Information	Health Care Information	High	High	High	High
1.1.1.88 Health Care Information	Health Care Information	High	High	High	High
1.1.1.89 Health Care Information	Health Care Information	High	High	High	High
1.1.1.90 Health Care Information	Health Care Information	High	High	High	High
1.1.1.91 Health Care Information	Health Care Information	High	High	High	High
1.1.1.92 Health Care Information	Health Care Information	High	High	High	High
1.1.1.93 Health Care Information	Health Care Information	High	High	High	High
1.1.1.94 Health Care Information	Health Care Information	High	High	High	High
1.1.1.95 Health Care Information	Health Care Information	High	High	High	High
1.1.1.96 Health Care Information	Health Care Information	High	High	High	High
1.1.1.97 Health Care Information	Health Care Information	High	High	High	High
1.1.1.98 Health Care Information	Health Care Information	High	High	High	High
1.1.1.99 Health Care Information	Health Care Information	High	High	High	High
1.1.1.100 Health Care Information	Health Care Information	High	High	High	High

**Table 2-2: Security Impact Level**

Security Objective	Impact Level
Confidentiality	High
Integrity	High
Availability	High

Note: Please refer to FIPS 199 Standards for Security Categorization

**PROPRIETARY AND CONFIDENTIAL**

Page 11

Figure 15: Automating System Security Plan



TrustedAgent enables risk tolerance to be defined at control level and be based on specific control templates defined for the standard or regulation (by default, the control templates deployed are preset with risk level of Moderate). Risk tolerance may also be impacted based by the compliance maturity of the organization. As required, the organization may also adjust the actual risk level of the implemented control to commensurate to applicable risks, the extent of impact, and control implementation.

Control Risk			Vulnerability Level		
Control:	ID-AM-4		Exploitability:	3	
Risk Score:	24		Objective Countermeasure:	2	
Risk Level:	Moderate		Actual Countermeasure:	0.0	
Risk Level = Vulnerability Score x Threat Score x Impact Score					
Risk Level	Risk Score (Min)	Risk Score (Max)	Vulnerability Score:	3	
Low	0	18	Vulnerability Level:	Moderate	
Moderate	19	54	Vulnerability Level = Exploitability - Actual Counter Measures		
High	55	Unlimited	Vulnerability Level	Vulnerability Score (Min)	Vulnerability Score (Max)
			Low	1	2
			Moderate	3	3
			High	4	5

Threat Level			Impact Level		
Capability:	2		Loss of Life:	0	
History:	2		Top Secret:	0	
Gain:	2		Confidential:	0	
Attributability:	1		Privacy Data:	0	
Detectability:	1		Operational:	2	
Threat Score:	4		Equipment Loss:	0	
Threat Level:	Moderate		Impact Score:	2	
Threat Level = Capability + History + Gain + Attributability + Detectability					
Threat Level	Threat Score (Min)	Threat Score (Max)	Impact Level:	Moderate	
Low	1	2	Impact Level = Loss of Life + Top Secret + Confidential + Privacy Data + Operations Impact + Equipment Loss		
Moderate	3	4	Impact Level	Impact Score (Min)	Impact Score (Max)
High	5	6	Low	1	1
			Moderate	2	3
			High	4	Unlimited

**Figure 16: Control Risk Management**

## 5 ASSESS Phase

Controls are assessed by independent assessors. Security Assessment Results (SAR), and other organizational documents can be utilized and tailored by system owners for their information systems. Findings are recorded and discussed with system owners. Findings are accepted and converted to corrective actions where they are tracked for remediation purposes.

Control assessment leverages standardized-industry test cases to assist organizations to determine the effectiveness of their controls. Custom test cases can also be supported to address any unique design considerations or regulation-specific requirements. Use of third-party assessor using a role-based interface within TrustedAgent is fully supported to ensure independent review of the assessment process. Privacy assessments can also be performed using NIST or HIPAA privacy controls or by using a privacy risk management framework consisting of privacy threshold analysis (PTA) and privacy impact assessment (PIA).

Regulations or Standards	Requirements	
COBIT ISO 27001	A.6.1.8: Independent review of information security A.6.2: External parties - To maintain the security of the organization's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties (A.6.2.1 thru. A.6.2.3) A.12.6.1: Control of technical vulnerabilities	MEA01: Monitor, Evaluate and Assess Performance and Conformance MEA02: Monitor, Evaluate and Assess the System of Internal Control MEA03: Monitor, Evaluate and Assess Compliance with External Requirements
ARS FISMA MARS-E	CA-2: Security Assessments CA-8: Penetration Testing PM-12: Threat Awareness Program	PM-14: Testing, Training, and Monitoring RA-3: Risk Assessment RA-5: Vulnerability Scanning
HIPAA HITECH Meaningful Use	§164.308(a)(8): Evaluation. Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that established the extent to which an entity's security policies and procedures meet the requirements of this subpart. → Conduct Evaluation.	
NIST CSF	ID.BE-1: The organization's role in the supply chain and is identified and communicated. ID.BE-5: Resilience requirements to support delivery of critical services are established. ID.RA-1: Asset vulnerabilities are identified and documented. DE.AE-2: Detected events are analyzed to understand attack targets and methods. DE.DP-2: Detection activities comply with all applicable requirements. DE.DP-3: Detection processes are tested.	
NERC CIP	CIP-003: Security Management Controls	
PCI DSS	6.1: Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities. 10.6.2: Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment. 11.2: Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades). 12.2 Implement a risk-assessment process that: <ul style="list-style-type: none"> <li>Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.),</li> <li>Identifies critical assets, threats, and vulnerabilities, and</li> <li>Results in a formal risk assessment.</li> </ul> A.1: Protect each entity's (that is, merchant, service provider, or other entity) hosted environment and data, per A.1.1 through A.1.4. A hosting provider must fulfill these requirements as well as all other relevant sections of the PCI DSS.	
SANS Critical Security Controls	CSC-4: Continuous Vulnerability Assessment and Remediation CSC-17-3: Perform an assessment of data to identify sensitive information that requires the application of encryption and integrity controls. CSC-20: Penetration Tests and Red Team Exercises	

### Figure 17: Control Assessment

### Figure 18: Control Assessment Details

16

Inventory										
View By: User Access   POCs   Interconnections   Inventory   Subsystems										
	Name	Parent Entity	Parent Asset	Type	Vendor	Product	Version	Hostname(s)		
VS-CMC1-IM	Not Applicable	VS-CMC1	Software	EMC	EMC Vileware					
VS-CMC1	Not Applicable	Not Applicable	Hardware	Dell	HP ProLiant sdx1770z g5					
VS-CMC2-IM	Not Applicable	VS-CMC2	Software	EMC	EMC Vileware					
VS-CMC2	Not Applicable	Not Applicable	Hardware	Dell	HP ProLiant sdx1770z g5					
VS-CMC1-OS	Not Applicable	VS-CMC1	Operating System	Microsoft	Microsoft Windows Server 2008 x64 (64-bit)		x64			
VS-CMC1-AppSrv	Not Applicable	VS-CMC1	Software	IBM	IBM WebSphere Commerce 7.0		7.0			
VS-CMC1-VCE	Not Applicable	VS-CMC1	Software	VirtualShopping.com	Virtual Commerce Engine		10.1	www.virtualshopping.com		
VS-CMC2-OS	Not Applicable	VS-CMC2	Operating System	Microsoft	Microsoft Windows Server 2008 x64 (64-bit)		x64			
VS-CMC2-DBSrv	Not Applicable	VS-CMC2	Database	Oracle	Oracle Database Server 11g 11.2.0.1.0 Enterprise Edition		11.2.0.1.0	ordbvr.virtuance.net		
VS-CMC1-GPE_GWY	Not Applicable	VS-CMC1	Software	Global Payment Services	Global Payment Services EngGateway		11	vs-enggateway-3545.gps-services.net		
VS-CMC1-FW1	Not Applicable	VS-CMC1	Hardware	Cisco	Cisco PIX Firewall 535					
VS-CMC2-FW1	Not Applicable	VS-CMC2	Hardware	Cisco	Cisco PIX Firewall 535					
shq-win08-03	Not Applicable	VS-CMC1	Software	Tenable	Tenable Nessus 5.2.1		5.2.1	shq-win08-03		
shq-win08-05	Not Applicable	VS-CMC1	Other	Microsoft	Microsoft Exchange Server 2010 for x64 based systems		2010	shq-win08-05		
baracoda	Not Applicable	VS-CMC1	Other	BaracodaOnline	BaracodaOnline 5.7.2		5.7.2			
shq-win08-02	Not Applicable	Not Applicable	Other	Other				shq-win08-02		

Figure 19: Asset Inventory

Hardware Assets										
Rows per page: 100 Total rows: 71										
#	Entity Name	Name	Type	Vendor	Product	Ver				
1	VirtualShopping.com	VS-CMC1	Hardware	Dell	HP ProLiant sdx1770z g5	0	0	0	0	0
2	VirtualShopping.com	VS-CMC1-FB1	Hardware	Cisco	Cisco PIX Firewall 535	0	1	0	1	0
3	VirtualShopping.com	VS-CMC2	Hardware	Dell	HP ProLiant sdx1770z g5	0	0	0	0	0
4	VirtualShopping.com	VS-CMC2-FB1	Hardware	Cisco	Cisco PIX Firewall 535	0	0	0	0	0
5	ACh Assessment Year 2013	Ta-ZCA1	Hardware	Dell	Dell ProLiant DAX	7.1	1	0	1	0
6	Baracoda Business Data Center	BARCDA-T1-ZCA1	Server	HP	HP ProLiant BL150 G5	5.5	1	0	1	0
7	Baracoda Business Data Center	BARCDA-T1-ZCA2	Server	HP	HP ProLiant BL150 G5	3.9	1	0	1	0
8	Patent Privacy Review1	PRIS-OS-GFW1	Hardware	Dell	Dell 3000m	0	0	0	0	0
Operating System Assets										
Rows per page: 100 Total rows: 47										
#	Entity Name	Name	Vendor	Product	Ver	Parent Entity	Parent Asset			
7	Patent Privacy Review1	PRIS-OS-GFW1_OS	Microsoft	Microsoft Windows Server 2008 x64 (64-bit)	x64	Not Applicable	PRIS-OS-GFW1	0	1	0
8	Patent Privacy Review1	PRIS-OS-GFW2_OS	Microsoft	Microsoft Windows Server 2008 x64 (64-bit)	x64	Not Applicable	PRIS-OS-GFW2	0	0	0
9	EPH Review Demo1	EPH-AK-ZCA1_OS	Microsoft	Microsoft Windows Server 2008 x64 (64-bit)	x64	Not Applicable	EPH-AK-ZCA1	6.3	1	0
10	EPH Review Demo1	EPH-AK-ZCA2_OS	Microsoft	Microsoft Windows Server 2008 x64 (64-bit)	x64	Not Applicable	EPH-AK-ZCA2	6.3	1	0
Software Assets										
Rows per page: 100 Total rows: 97										
#	Entity Name	Name	Vendor	Product	Ver	Parent Entity	Parent Asset			
22	Patent Privacy Review1	PRIS-OS-GFW1-TrustAgent	TrustedAgent GRC	TrustedAgent GRC	5.0.3	Not Applicable	PRIS-OS-GFW1	0	0	0
23	Patent Privacy Review1	PRIS-OS-GFW1-IM	EMC	EMC Vileware	Not Applicable	Not Applicable	PRIS-OS-GFW1	0	1	0
24	Patent Privacy Review1	PRIS-OS-GFW2-IM	EMC	EMC Vileware	Not Applicable	Not Applicable	PRIS-OS-GFW2	0	0	0
25	Patent Privacy Review1	essus@vileware.com	Ever	Ever Retina 5.10.12.1700	Not Applicable	Not Applicable	Not Applicable	10	15	0
26	EPH Review Demo1	EPH-AK-ZCA1-Java Server	Apache	Apache Software Foundation Tomcat	Not Applicable	Not Applicable	EPH-AK-ZCA1	6.4	1	0
27	EPH Review Demo1	EPH-AK-ZCA1-TrustAgent	TrustedAgent GRC	TrustedAgent GRC	5.0.3	Not Applicable	EPH-AK-ZCA1	0	0	0
28	EPH Review Demo1	EPH-AK-ZCA1-IM	EMC	EMC Vileware	Not Applicable	Not Applicable	EPH-AK-ZCA1	5.5	1	0
29	EPH Review Demo1	EPH-AK-ZCA2-IM	EMC	EMC Vileware	Not Applicable	Not Applicable	EPH-AK-ZCA2	0	0	0

Figure 20: Vulnerabilities by Risk Level and Asset Group

TrustedAgent enables vulnerabilities to be organized into easy to understand finding reports along with risk level and remediation status, and provides the details for end-users to view the vulnerabilities online without the complexity of XML as identified by the vulnerability scanning tools.

Identification
People and Inventory
Controls
Findings
Authorization
Reports

Findings

Rows per page:
25
Total rows: 5

View By:
Findings By List
Findings By Reports
Corrective Actions

	Report ID	Date	Title	#	Risk Level				Remediation Status			
New					H	M	L	I	U	A	R	C
	RETINA-2014-06-08 14:01:23.697	2014-06-08	RETINA-Scanner Results	0	0	0	0	0	0	0	0	0
	VS-PCI-2014	2014-06-01	QSA LLC Baseline 2014 Audit	3	0	2	1	0	0	3	0	0
	NEXPOSE-2014-06-08 13:58:40.896	2012-10-09	NEXPOSE-Scanner Results	0	0	0	0	0	0	0	0	0
	NESSUS-2014-06-08 14:00:51.243	2012-03-22	NESSUS-Scanner Results	10	0	9	1	0	3	2	2	3
	NESSUS-2014-06-08 14:09:18.834	2012-03-22	NESSUS-Scanner Results	1	1	0	0	0	0	1	0	0

Figure 21: Finding Reports

Identification | People and Inventory | Controls | **Findings** | Authorization | Reports

**Findings**

### 1.0 Overview

This document contains a summary and detailed listing of the findings identified in the report below. The document provides a Finding Summary view (chapter 2) and Finding Details view (chapter 3). The summary view shows the findings grouped by affected assets and risk levels. The details View contains detailed description, risk analysis, and affected asset information for each finding grouped by asset name.

Report ID:	RETINA-2014-01-17 13:44:37.555
Title:	Retina Scanner Results
Date:	01/17/2014
Description:	Retina Scanner Results

### 2.0 Finding Summary

This chapter contains a summary of the findings from the identified report. The findings are grouped by the affected asset, risk levels and current remediation status.

Asset	Subtotal	Risk Level				Remediation Status			
		High	Moderate	Low	Informational	Unlinked	Active	Rejected	Completed
EPHI-AK-ZCA1-OS	1	0	1	0	0	0	1	0	0
EPHI-AK-ZCA1-VM	1	0	1	0	0	0	1	0	0
EPHI-AK-ZCA2	3	2	0	1	0	1	1	1	0
EPHI-AK-ZCA1-App Server	1	1	0	0	0	0	1	0	0
EPHI-AK-ZCA2-DB Server	2	1	0	1	0	0	1	1	0
EPHI-AK-ZCA1	2	1	1	0	0	2	0	0	0
EPHI-AK-ZCA2-OS	1	1	0	0	0	0	0	1	0
<b>Total:</b>	<b>11</b>	<b>6</b>	<b>3</b>	<b>2</b>	<b>0</b>	<b>3</b>	<b>5</b>	<b>3</b>	<b>0</b>

### 3.0 Finding Details

This chapter contains a detailed listing of the findings identified in the identified report. The findings are grouped by their risk levels.

### 3.1 Asset Name: EPHI-AK-ZCA1

#### 3.1.1 Seagate Embedded Driver Multiple Vulnerabilities (2681578) - .NET - 2656411

**Risk Level: High** **CVSS: 9.3**

**Remediation Status**

**Status:** Unlinked

**General Information**

Seagate Embedded Driver contain multiple vulnerabilities when processing crafted TypeType font files (.ttf), EMF record types and embedded images, Windows and Messages, Keyboard Layout files, Scrollbars, and crafted .NET applications. Successful exploitation could allow an attacker to elevate their privileges, create denial of service conditions, and execute arbitrary code remotely with elevated privileges via multiple vectors.

**Detailed Information**

[Back to Summary](#) [Back to Top](#)

#### 3.1.2 GPU-Accelerated CHIP supporting Adobe Products Multiple Vulnerabilities (20120328) - Adobe AIR x64

**Risk Level: Moderate** **CVSS: 6.2**

**Remediation Status**

**Status:** Unlinked

**General Information**

Adobe products (Flash, AIR) contain multiple vulnerabilities when handling URL security domain checking and unspecified vectors related to the NetStream class. Successful exploitation may result in arbitrary code execution impacting certain GPU chipsets.

**Detailed Information**

**Corrective Control**

Ensure that Adobe products are patched as required.

**Impact Analysis**

Category II

**Risk Management**

**Likelihood:** Moderate

Figure 22: Online View of Finding Report

Identification | People and Inventory | Controls | **Findings** | Authorization | Reports

### Vulnerability Assessment Interval

Exclude from Scan: ☒

Scheduled Scan Dates: Start Date: 06/11/2014 End Date: 06/11/2014

Scan Interval: ☐ Weekly ☒ Monthly ☐ Annually

Recur on day 1 of every 1 month(s)

Scan Immediately on Next Scheduled Run: ☐

### Incident Management

Handler for Incident Reported: ☐

### Assets to Scan

Assets to Scan (hold down CTRL for multiple select/deselect):

- VS-CMC1-VM
- VS-CMC1
- VS-CMC2-VM
- VS-CMC2
- VS-CMC1-OS
- VS-CMC1-AppSvr
- VS-CMC1-VCE
- VS-CMC2-OS
- VS-CMC2-DBSvr
- VS-CMC1-GPS\_GWY

Figure 23: Integrated Vulnerability Management

TrustedAgent will also automate the reporting of the vulnerabilities into the SAR by asset and risk level along with any identified corrective actions, thereby eliminates the burden of having to manually cut and paste the details from vulnerabilities report and to map to the impacted assets. The SAR template is highly flexible allowing unique organization-features be incorporated by the organization. In addition, the SAR may also contain:


- List of non-conforming controls
- Use of compensating controls
- Risks from interconnections
- Risk distribution/summary along with in-progress corrective actions

Security Assessment Report  
EPHI Review Demo1

May 14, 2014

Version Revision

**EPHI Review Demo1**  
(ePHI-Demo1)





**Security Assessment Report**  
**EPHI Review Demo1**

Version Revision

May 14, 2014

PROPRIETARY and CONFIDENTIAL

PROPRIETARY and CONFIDENTIAL

Page 1

Security Assessment Report  
EPHI Review Demo1

May 14, 2014

Version Revision

**6.0 Authorization Recommendation**  
A total of 17 system risks were identified for EPHI Review Demo1. The risks identified from the system are summarized in Table 6-1 along with the recommended remediation priority (1=highest, most urgent to 3=lowest, least urgent).

**Table 6-1: Risk Summary Distribution**

Priority	Risk Level	Count	Active	Unlinked	Rejected	Completed
1	High Risks	7	3	2	2	0
2	Moderate Risks	7	2	4	0	1
3	Low Risks	3	1	1	1	0
	<b>Total Risks</b>	<b>17</b>	<b>6</b>	<b>7</b>	<b>3</b>	<b>1</b>

The organization should take the above identified risks into consideration in the development of a Plan of Corrective Action and Milestones for EPHI Review Demo1. The Plan is a remediation and mitigation plan designed to address specific residual security weaknesses, cost and resources required, activities (milestones) to be taken, and by whom, and key target dates. The implementation of the plan is the responsibility of the organization's that owns and operates EPHI Review Demo1 and the assigned corrective action and milestone owners.

Table 6-2 indicates any specific additional guidance from the assessor including risk level and the priority of recommended risk mitigation actions for the EPHI Review Demo1.

**Table 6-2: Risk Mitigation Priorities**

Priority Number	Risk Level	Identifier	Vulnerability Description
1			
2			
3			
4			
5			
6			
7			

PROPRIETARY and CONFIDENTIAL

Page 42

Security Assessment Report  
IT Security Management Demo1

June 26, 2014

Version Revision

Table 4-2: Security Assessment Results for Database Scan

ID	Title	Source of Discovery	Risk Statement	Vulnerability IDs	Affected Asset	Impact	Likelihood	Risk Exposure	Recommended Corrective Action
No items found									

Table 4-3 Security Assessment Results for Web Application Scan

ID	Title	Source of Discovery	Risk Statement	Vulnerability IDs	Affected Asset	Impact	Likelihood	Risk Exposure	Recommended Corrective Action
15	Poison Null Byte Windows Files Retrieval	Vulnerability Assessment	This issue may affect different types of products.	atnNullByte (http://demo.testfire.net/default.aspx)	watchfire appscan server 2	High	High	High	

Table 4-4: Security Assessment Results for Other Scan & Misc. Testing Scan

ID	Title	Source of Discovery	Risk Statement	Vulnerability IDs	Affected Asset	Impact	Likelihood	Risk Exposure	Recommended Corrective Action
1	Access Control Enforcement	Security Assessment	Gap in process	T-24		Moderate	Moderate	Moderate	Review the gaps of existing access control enforcement and implement the required control elements.
53	Test CGI Finding	Security Assessment				High	Moderate	Moderate	
3	Separation of Duties	Security Assessment	Gap in overall process.	T-1,T-16,T-24		Moderate	Low	Low	Update the review policy for Active Directory to include review of group policies
2	Information Flow Enforcement	Security Assessment	Gap in overall process.	T-24, T-36		Low	Moderate	Low	Revise the information flow review and approval process.

PROPRIETARY and CONFIDENTIAL

Page 29

Figure 24: Sample Security Assessment Output with Integrated Vulnerability Reporting



## 6 MANAGE Phase

Incidents or issues identified by internal or external parties (such as customer complaints, data breaches, security or privacy incidents) can also be tracked and managed as findings. Findings are either accepted or rejected by system owners according to organization policies/procedures. Corrective actions (CAPs), or remediation plans, may be created for findings that are not Fully Satisfied, and where risks have not been accepted by the authorizing official, or have legal or regulatory consequences if not addressed.

Regulations or Standards	Requirements
COBIT ISO 27001	A.13.1.1: Reporting information security events A.13.1.2: Reporting security weaknesses APO10: Manage Suppliers APO12: Manage Risk
ARS FEDRAMP FISMA MARS-E	CA-5: Plan of Action and Milestones
HIPAA HITECH Meaningful Use	164.530(f): Mitigation. A covered entity must mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of this subpart by the covered entity or its business associate. → Mitigate known harmful effects from violations of its P&Ps and the Privacy Rule by its workforce and business associates.
NIST CSF	ID.RA-3: Threats, both internal and external, are identified and documented. ID.RA-4: Potential business impacts and likelihoods are identified. ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk. ID.RA-6: Risk responses are identified and prioritized.
NERC CIP	CIP-003: Security Management Controls.
PCI DSS	6.1: Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities. 6.5.6: All "high risk" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1).
SANS Critical Security Controls	CSC-4: Continuous Vulnerability Assessment and Remediation

Through risk mitigation discussion with entity's business owner and oversight staff, findings exceeding risk tolerance defined for the organization, or regulatory specific findings from regulator audits can be accepted for remediation using corrective actions. The remaining findings (threshold below organization's risk tolerance) can be risk-accepted and rejected through justifications.

Finding Details	
<b>Finding Information</b>	
<b>General Information</b>	
Number:	1 <a href="#">Edit</a>
Finding Type:	Security Assessment
Finding Report:	2014-Q2-AA
Recommendation Number:	
Title:	Interconnections to External Systems are not Current
Finding:	Interconnections related to VOIP to MegaPath are not maintained as part of the inventory of critical services.
<b>Detailed Information</b>	
Detailed Description:	
Corrective Action:	Update the interconnections and track the additional interconnections within TrustedAgent GRC.
Known Exploit:	MegaPath Server default admin account is well known to be exploited.
Impact Analysis:	Path for any weakness to be exploited
Reference:	
<b>Associated Control</b>	
Link to Control:	<a href="#">ID-AM-3 Organizational Interconnections and Data Flows</a>
Test Results:	QSA LLC noted during review of the control implementation that the interconnections leveraged by the organization are not current. Key infrastructure such as VOIP were not included in the analysis.
<b>Remediation Status</b>	
Status:	Unlinked <a href="#">Accept Link</a>
Justification / Comment:	
Actual Completion Date:	
<b>Risk Management</b>	
CVSS:	0.0 <a href="#">Edit</a>
CWSS:	0.0
Initial Severity:	Moderate
Likelihood:	Moderate
Impact:	High
Risk Level:	Moderate
<b>Affected Asset Information</b>	
Associated Asset:	Not Applicable <a href="#">Edit</a>
CVE:	
CWE:	
CCE:	
STIG:	
Vulnerability ID:	T-35

Figure 25: Finding Identification and Analysis

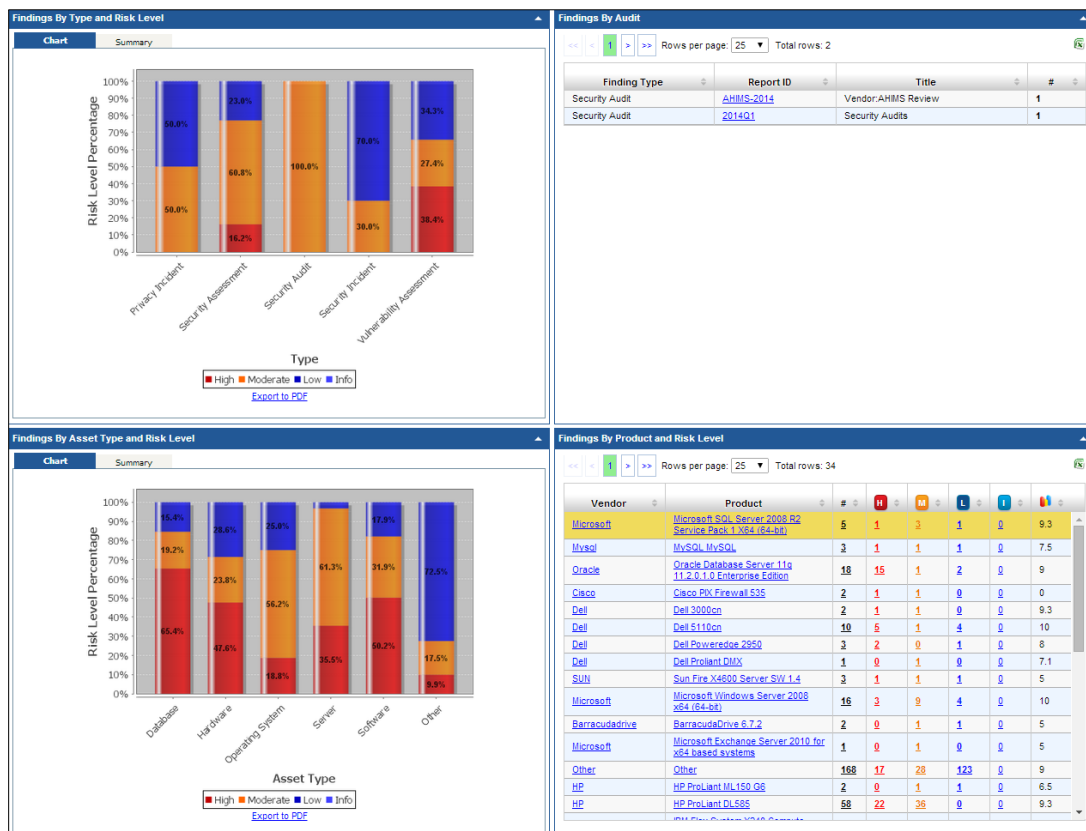


Figure 26: Findings by Type, Risk Level, and Product Group

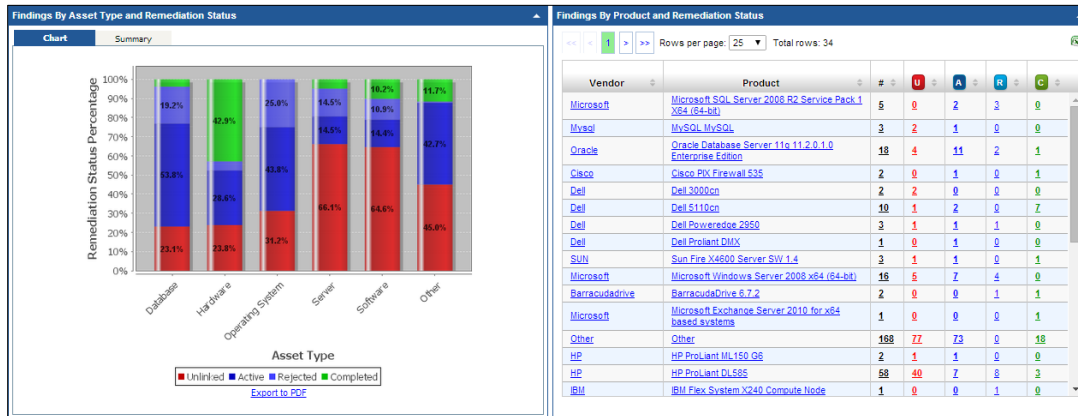


Figure 27: Findings by Remediation Status and Product Group

Identification   People and Inventory   Controls   Findings   Authorization   Reports									
Corrective Actions Corrective Action: 4									
View By: Findings By List Findings By Reports Corrective Actions									
	Description	ID	Status	Risk	SCD	ECD	ACD	POC	
	Weakness to address Retina vulnerability scan issues.	Alaska-ePHI-Demo1_Q2_2014_1	Delayed	Moderate	2014-05-17	2014-05-17	TBD	Tuan Phan, tuanp@trustedintegration.com	
	Microsoft Windows, Office, .NET Framework, and Silverlight contain multiple vulnerabilities when processing crafted TypeType font files (TTF, EMF re (...more)	ePHI-Demo1_Q3_2014_3	In Progress	High	2014-07-31	2014-07-31	TBD	Tuan Phan (HQ), tuanp@trustedintegration.com	
	Organization needs to review and update its CP policy and procedures.	ePHI-Demo1_Q3_2014_4	In Progress	Moderate	2014-07-31	2014-07-31	2014-07-31	Tuan Phan (HQ), tuanp@trustedintegration.com	

Figure 28: Corrective Action Summary

In addition to addressing findings as the results of security control assessment or external regulatory or audit bodies, TrustedAgent's incident and finding management capabilities enable organizations to identify security and privacy incidents, conduct impact analysis to derive risk level, manage remediation, and report/share incident reports to regulatory or industry bodies.

Regulations or Standards	Requirements	
COBIT ISO 27001	A.13.1.1: Reporting information security events A.13.1.2: Reporting security weaknesses A.13.2.3: Collection of evidence APO12: Manage Risk APO13: Manage Security	DSS02: Manage Service Requests and Incidents DSS03: Manage Problems DSS04: Manage Continuity DSS05: Manage Security Services
ARS FISMA MARS-E	IR-4: Incident Handling IR-5: Incident Monitoring IR-6: Incident Reporting IR-8: Incident Response Plan	
HIPAA HITECH Meaningful Use	§164.308(a)(6)(ii): Security Incident Procedures. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes. → Develop and Implement Procedures to Respond to and Report Security Incidents. Incorporate Post-Incident Analysis into Updates and Revisions. §164.404 to §164.410: Notification to Individuals, Media, Secretary of HHS and Business Associates.	
NIST CSF	DE.AE-4: Impact of events is determined. DE.AE-5: Incident alert thresholds are established. RS.AN-1: Notifications from the detection system are investigated. RS.AN-2: The impact of the incident is understood. RS.AN-4: Incidents are classified consistent with response plans.	

Regulations or Standards	Requirements
NERC CIP	CIP-008-5: Incident Reporting and Response Planning: <ul style="list-style-type: none"> <li>• R1: Cyber Security Incident Response Plan</li> <li>• R2: Implementation and testing of Cyber Security Incident Response Plans</li> <li>• R3: Cyber Security Incident Response Plan Review, Update and Communication</li> </ul>
PCI DSS	12.10: Implement an incident response plan. Be prepared to respond immediately to a system breach. 12.10.1: Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses minimum requirements. 12.10.3: Designate specific personnel to be available on a 24/7 basis to respond to alerts. 12.10.5: Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems. 12.10.6: Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.
SANS Critical Security Controls	CSC-18: Incident Response and Management

Incidents identified by internal or external reporting personnel may be documented in TrustedAgent through an incident handler such as an Incident Management Program. The reporting form is designed to meet the requirements of US-CERT, HHS Incident Reporting and Breach Notification, and ISAC groups. Findings are automatically created for each reported incident to ensure all reported incidents are properly reviewed and handled.

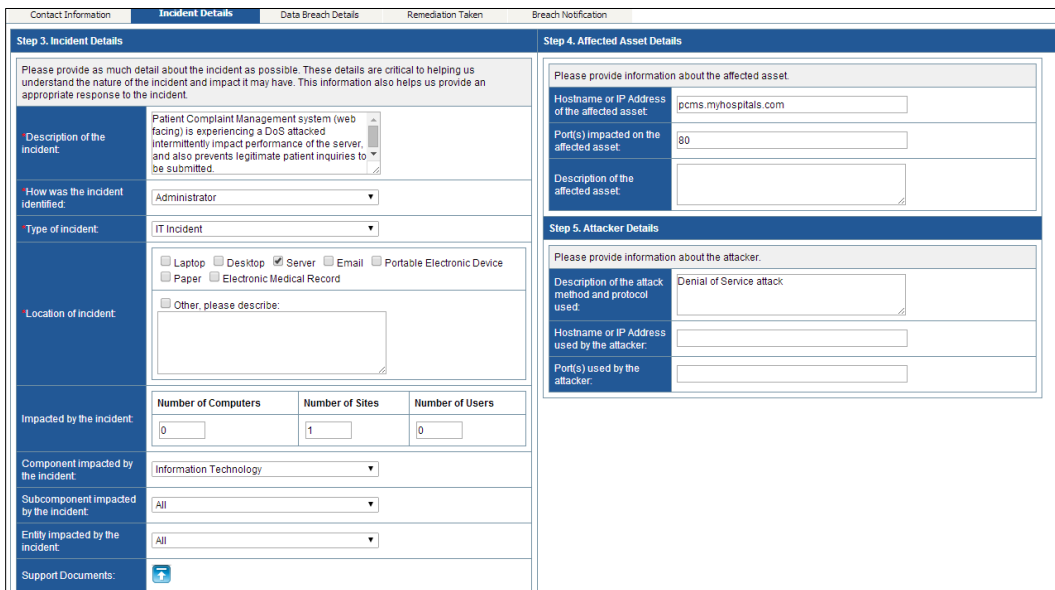


Figure 29: Incident Identification and Reporting

<a href="#">New</a>	<a href="#">Edit</a>	<a href="#">Delete</a>	Submission Date	Incident ID	Description	Status	Submitted By	First Name	Last Name
			2014-05-12 00:00:00	TA20140512.172752.8	Patient Complaint Management system (web facing) is experiencing a DoS attacked intermittently impact performance of the server, and also prevents legitimate patient inquiries to be submitted.	Unknown	tpa_hq	Jim	Baker
			2014-05-07 00:00:00	TA20140507.090125.7	My medical records were found in a dumpster behind 7-11	Occurring	tphan	John	Roberts
			2014-04-23 00:00:00	TA20140423.124756.6	First level window was broken and a laptop, file cabinet, and binders were taken from 3 offices.	Occurring	opmuser	John	Smith
			2014-04-15 00:00:00	TA20140415.194822.5	My laptop was stolen from my car parked at the local mall.	Occurring	tphan	Quynh	Nguyen

Figure 30: List of Incidents



Figure 31: Incident Metrics

By leveraging the finding and incident dashboard views organization can obtain in-depth understanding of the risks impacting the organization to better position resources to mitigate and remediate the risks. Legal and obligatory notifications to impacted individuals, media, law enforcement, regulators, or industry groups can also be documented as well as real-time notifications to ensure compliance and remediation activities are timely addressed.


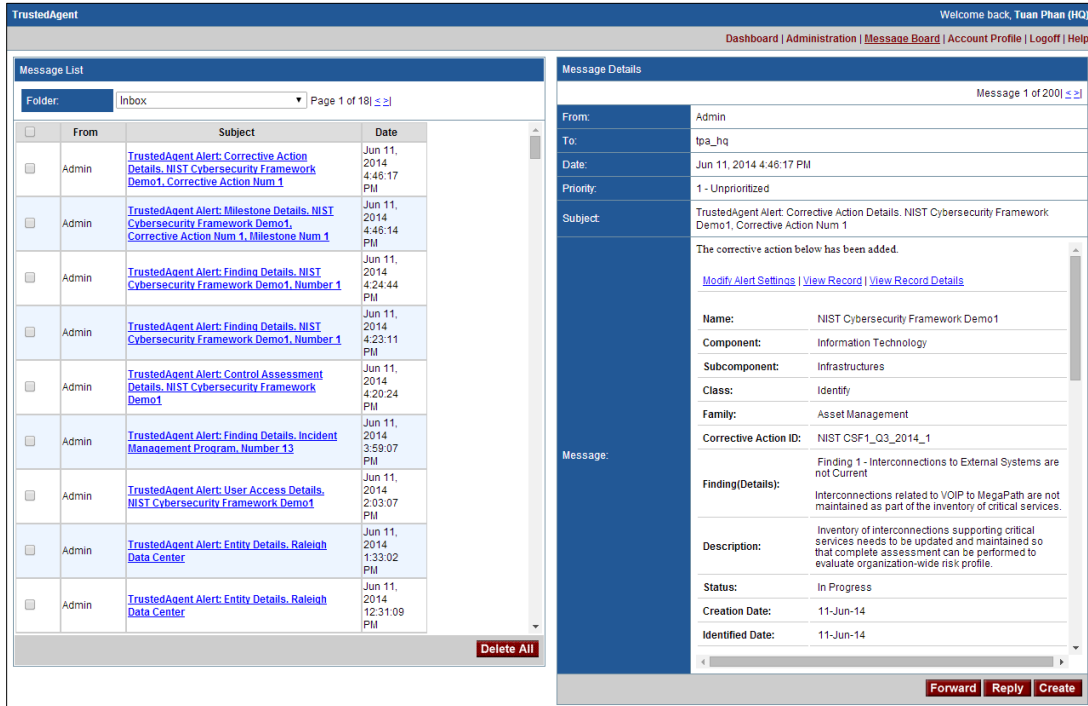
Contact Information	Incident Details	Data Breach Details	Remediation Taken	Breach Notification
<b>Step 8: Breach Notification</b>				
<div>Individuals</div> <div>Media</div> <div>Law Enforcement</div> <div>Information Sharing</div> <div>Regulatory</div>				
Please provide any notifications that have been taken to report the breach to affected individuals.				
Individual Notice Provided:		Yes		
Individual Notice Dates:		Start Date	End Date	
		06/09/2014 12:00:00 AM	06/13/2014 12:00:00 AM	
Substitute Notice Provided:		No		
Support Documents:				

Figure 32: Incident Notifications



The screenshot displays the TrustedAgent Message Board. The left pane shows a list of messages from 'Admin' with subjects related to 'TrustedAgent Alert: Corrective Action Details' and 'TrustedAgent Alert: Finding Details'. The right pane shows the details of a selected message, including the finding description: 'Finding 1 - Interconnections to External Systems are not Current' and the corrective action: 'Interconnections related to VOIP to MegaPath are not maintained as part of the inventory of critical services.'

Figure 33: Message Board Notifications

## 7 AUTHORIZE Phase

The authorization package is presented to the authorizing official for review and approval. Approval letters and waivers, including Authority to Operate (ATO) and Attestation of Compliance (AOC), are created from predefined templates that document the accreditation decision for the entity along with residual risks that was accepted and granted. Assessment and authorization security metrics (i.e., statuses, dates, and approvals) are recorded for the entity. Key artifacts supporting compliance can be tracked and served as body of evidence of compliance.

Regulations or Standards	Requirements
COBIT ISO 27001	A.6.1.4: Authorization process for information processing facilities A.14.1.3: Developing and implementing continuity plans including information security
ARS FedRAMP FISMA MARS-E	CA-6: Security Authorization
HIPAA HITECH Meaningful Use	164.308(a)(2): Assigned security responsibility. Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity. 164.308(a)(8): Evaluation. Perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.
NIST CSF	ID.BE-5: Resilience requirements to support delivery of critical services are established. PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed. PR.IP-12: A vulnerability management plan is developed and implemented



Regulations or Standards	Requirements
NERC CIP	CIP-003-5: Security Management Controls – R1, R2 CIP-009-5: Recovery Plans for BES Cyber Systems: <ul style="list-style-type: none"> <li>• R1: Cyber Security Incident Response Plan</li> <li>• R2: Implementation and testing of Cyber Security Incident Response Plans</li> <li>• R3: Cyber Security Incident Response Plan Review, Update and Communication</li> </ul>
PCI DSS	Self-Assessment Questionnaires (SAQ) and Attestation of Compliance (OAC) is signoff by senior company officer. Report of Compliance (ROC) is performed by Qualified Security Assessor (QSA).
SANS Critical Security Controls	<i>Recommended as best practices.</i>

For each of the organization's entities, authority to operate (ATO) letter, attestation of compliance, and other authorization documents can be issued for meeting the risks and requirements. Supporting documentation can subsequently be maintained with relevant performance metrics (expiration and test dates, status, supporting artifacts) and available on management dashboard for ongoing visibility and accountability.

**MEMORANDUM**

DATE: December 21, 2013  
TO: Director, CFPB  
FROM: Chief Information Officer and Director, CFPB  
SUBJECT: Accreditation Decision for the TTS Security Management System (TTSMS) System

**REPLY REQUESTED 30 DAYS FROM THE DATE OF THIS MEMORANDUM**

The TTS Security Management System (TTSMS) System is a standalone system.

The previous Authority To Operate (ATO) for TTSMS System, signed on 12/21/2013.

I have determined through a review of the certification package that the risk to CFPB information and CFPB information systems resulting from the operation of the TTSMS System is acceptably protected on the completion of the actions described in the Attachment. Accordingly, I am issuing an **Authorization To Operate (ATO)** for TTSMS System, valid 12/28/2014 in the existing operating environment. This security accreditation is my formal declaration that adequate security controls have been implemented in the information system and that a satisfactory level of security is present in the system. The security accreditation of the information system will remain in effect as long as: (i) the required security status reports for the system are submitted to this office no less than every three years; (ii) the vulnerabilities reported during the continuous monitoring process do not result in additional agency-level risk which is deemed unacceptable; and (iii) the system has not exceeded the maximum allowable time period between security accreditations in accordance with Federal or CFPB policy.

The actions set forth in the attachment must be addressed on or later than the designated completion date. This office will monitor the Plan of Action and Milestones (POA&M) submitted with the accreditation package during the period of authorization.

If you have questions, please contact

Name	George Wilson
Office	CFPB
Title	Chief Information Officer (CIO)
Organization	Department of Consumer
Address	1120 Wilson Arlington, VA 22204
Telephone	703-260-8171
Email	george.wilson@cfpb.gov

The CIO is the senior level executive within the organization responsible for the establishment and maintenance of the enterprise vision, strategy and processes to ensure

PROPRIETARY AND CONFIDENTIAL Page 1

Information assets are adequately protected. The CIO is responsible for identifying, analyzing, implementing and maintaining security controls to protect information assets in accordance with the information security policy. The CIO is responsible for ensuring that the information security policy is implemented and maintained in accordance with the information security policy.

Authorization decision is required for the following reasons:

Issue "X" to indicate selection	Authorization Decision Reason
<input type="checkbox"/> New System	
<input type="checkbox"/> Major system modification	
<input type="checkbox"/> Service security violation	
<input type="checkbox"/> Change in the threat environment	
<input type="checkbox"/> External information to report	

Payment Card Industry (PCI)  
Data Security Standard

**Attestation of Compliance for Onsite Assessments – Merchants**  
Version 3.0  
June 27, 2014

PCI DSS is a set of requirements designed to ensure that all companies that accept, process, store, or transmit payment card information maintain a secure system.

June 27, 2014 Page 1

Attestation of Compliance  
Version 3.0  
June 27, 2014

**Section 1: Assessment Information**

**Instructions for Submitters**

This Attestation of Compliance must be completed as a declaration of the results of the merchant's assessment with the Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS). Completion of this form is required for all merchants that accept, process, store, or transmit payment card information, as applicable. Contact your assessor (merchant bank) or the payment brand for reporting and submission procedures.

**Part 1: Service Provider and Qualified Security Assessor Information**

Company Name	Example Company	SAQ Type	SAQ Type
Company Type	Example Company	SAQ Type	SAQ Type
Company Address	Example Company	SAQ Type	SAQ Type
Company Phone	Example Company	SAQ Type	SAQ Type
Company Email	Example Company	SAQ Type	SAQ Type
Company Website	Example Company	SAQ Type	SAQ Type
Company Fax	Example Company	SAQ Type	SAQ Type
Company FIC	Example Company	SAQ Type	SAQ Type

**Part 2: Merchant Information**

Company Name	Example Company	SAQ Type	SAQ Type
Company Type	Example Company	SAQ Type	SAQ Type
Company Address	Example Company	SAQ Type	SAQ Type
Company Phone	Example Company	SAQ Type	SAQ Type
Company Email	Example Company	SAQ Type	SAQ Type
Company Website	Example Company	SAQ Type	SAQ Type
Company Fax	Example Company	SAQ Type	SAQ Type
Company FIC	Example Company	SAQ Type	SAQ Type

**Part 3: Description of Payment Card Business**

How and in what capacity does your business store, process, and/or transmit payment card data?

**Part 4: Location**

How and in what capacity does your business store, process, and/or transmit payment card data?

PROPRIETARY AND CONFIDENTIAL Page 2

Figure 34: Sample ATO Letter / Attestation of Compliance for PCI DSS

### Control Assessment

Security Assessment Plan Wizard

Security Authorization Executive Summary Wizard

Security Assessment Report Wizard

Status: Completed

Initiation Date: 01/17/2014

Estimated Completion Date: 01/17/2014

Last Completion Date: 01/17/2014

Expiration Date: 01/17/2015

Last Reviewed Date: 01/17/2014

Next Review Date: 01/17/2015

Last VA Date: 01/17/2014

VA Expiration Date: 01/17/2015

Next VA Date: 01/17/2015

New	Move	Num	Support Document	Uploaded Date	ISSM Validation	HQ Review
		1	<a href="#">Security Assessment Plan</a>	04/07/2014		
		2	<a href="#">Security Assessment Report</a>	04/07/2014		
		3	<a href="#">Security Authorization and Executive Summary</a>	01/17/2014		<span>In Progress</span>

### Contingency Plan

CP Wizard

CP Inherit Allow: ☐

Status: Completed

Is Completed or Tested?: Completed but Not Tested

Initiation Date: 01/17/2014

Estimated Completion Date: 01/17/2014

Last Completion Date: 01/17/2014

Expiration Date: 01/17/2015

Last Reviewed Date: 01/17/2014

Next Review Date: 01/17/2015

Last Test Date: 01/17/2014

Test Expiration Date: 01/17/2015

Next Test Date: 01/17/2015

New	Move	Num	Support Document	Uploaded Date	ISSM Validation	HQ Review
		1	<a href="#">Contingency Plan Artifact</a>	04/07/2014		
			Tested Contingency Plan Artifact		<span>Not Started</span>	<span>Not Started</span>

### System Security Plan

SSP Wizard

SSP Inherit Allow: ☐

Status: Completed

Initiation Date: 01/17/2014

Estimated Completion Date: 01/17/2014

Last Completion Date: 01/17/2014

Expiration Date: 01/17/2015

Last Reviewed Date: 01/17/2014

Next Review Date: 01/17/2015

New	Move	Num	Support Document	Uploaded Date	ISSM Validation	HQ Review
		1	<a href="#">SSP Artifact</a>	04/07/2014		

### Risk Assessment

RA Wizard

RA Inherit Allow: ☐

Status: Completed

Initiation Date: 01/17/2014

Estimated Completion Date: 01/17/2014

Last Completion Date: 01/17/2014

Expiration Date: 01/17/2015

Last Reviewed Date: 01/17/2014

Next Review Date: 01/17/2015

New	Move	Num	Support Document	Uploaded Date	ISSM Validation	HQ Review
		1	<a href="#">Risk Assessment Artifact</a>	04/07/2014		

Figure 35: Tracking Key Performance Metrics of Regulatory Reports

TrustedAgent supports customization of document templates and control libraries to meet regulatory reporting needs and for changes based on organization's requirements using the TrustedAgent Content Framework described below:

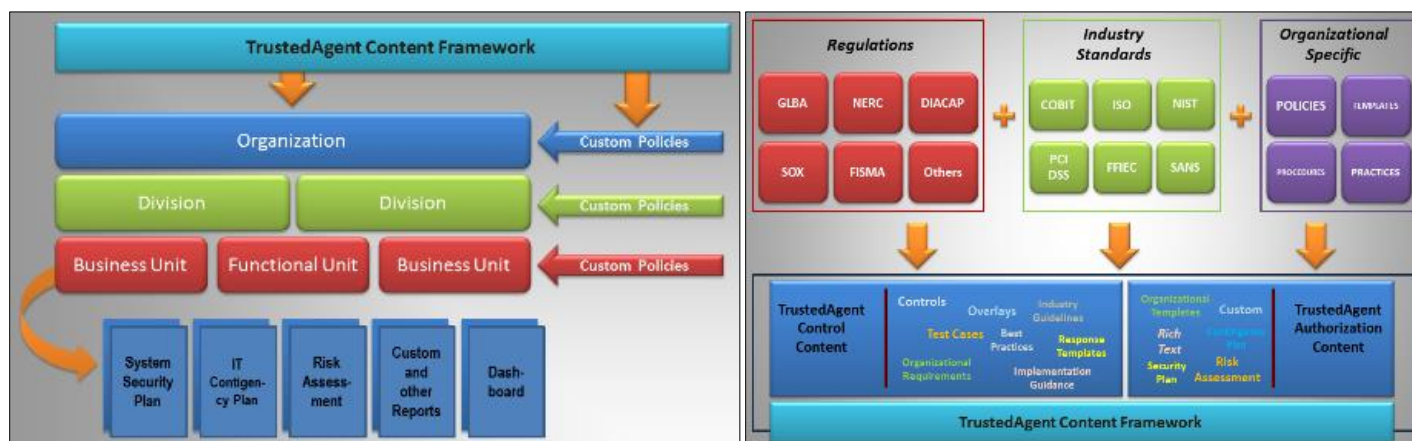
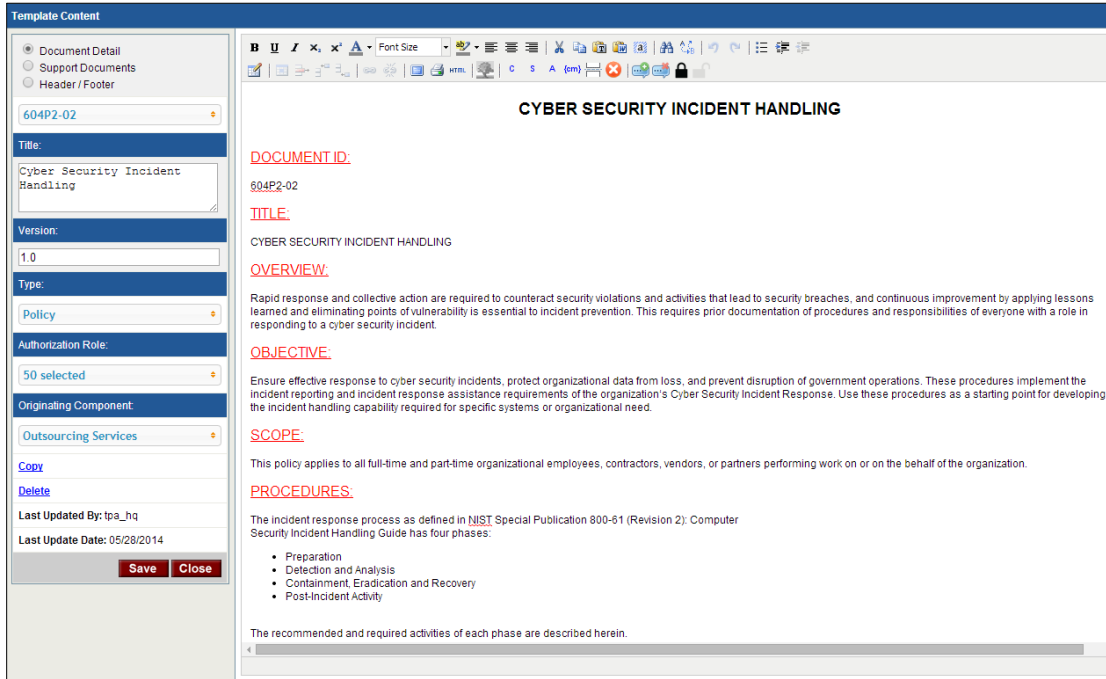


Figure 36: TrustedAgent Content Framework

For NIST cybersecurity framework, TrustedAgent provides generic incident response, vulnerability management plan, and business continuity policies, procedures, and plans for organizations to leverage to ensure rapid implementation. Additional or organization-specific policies and procedures can also be implemented and maintained:



**Template Content**

Document Detail  
Support Documents  
Header / Footer

604P2-02

Title:  
Cyber Security Incident Handling

Version:  
1.0

Type:  
Policy

Authorization Role:  
50 selected

Originating Component:  
Outsourcing Services

Copy  
Delete

Last Updated By: tpa\_hq  
Last Update Date: 05/28/2014

Save Close

**CYBER SECURITY INCIDENT HANDLING**

DOCUMENT ID:  
604P2-02

TITLE:  
CYBER SECURITY INCIDENT HANDLING

OVERVIEW:  
Rapid response and collective action are required to counteract security violations and activities that lead to security breaches, and continuous improvement by applying lessons learned and eliminating points of vulnerability is essential to incident prevention. This requires prior documentation of procedures and responsibilities of everyone with a role in responding to a cyber security incident.

OBJECTIVE:  
Ensure effective response to cyber security incidents, protect organizational data from loss, and prevent disruption of government operations. These procedures implement the incident reporting and incident response assistance requirements of the organization's Cyber Security Incident Response. Use these procedures as a starting point for developing the incident handling capability required for specific systems or organizational need.

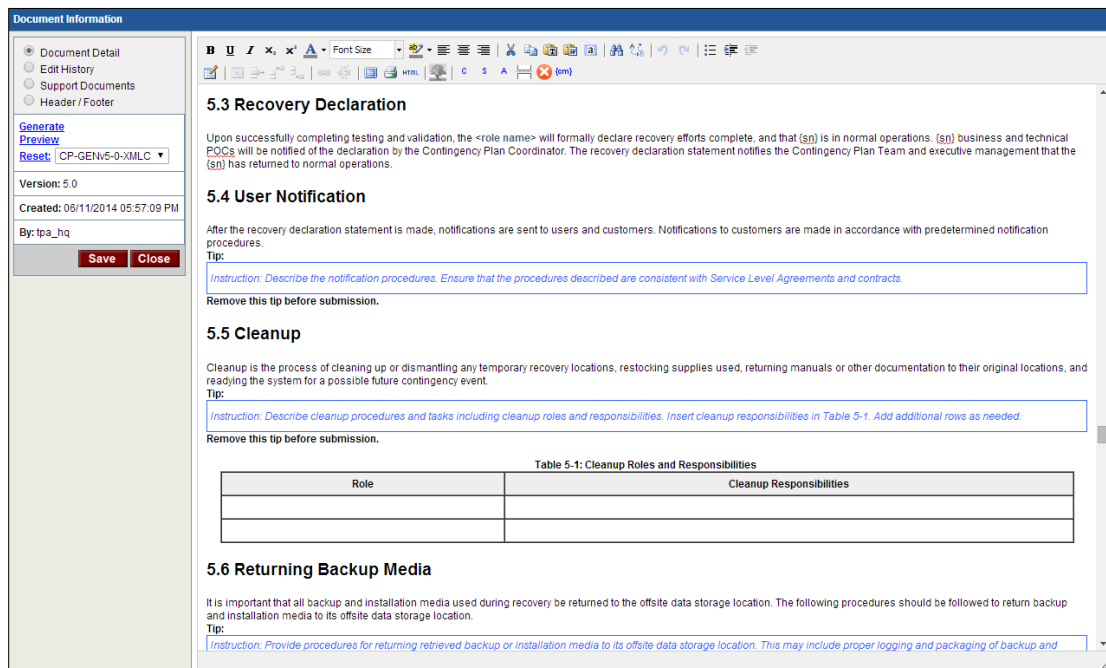
SCOPE:  
This policy applies to all full-time and part-time organizational employees, contractors, vendors, or partners performing work on or on the behalf of the organization.

PROCEDURES:  
The incident response process as defined in NIST Special Publication 800-61 (Revision 2): Computer Security Incident Handling Guide has four phases:

- Preparation
- Detection and Analysis
- Containment, Eradication and Recovery
- Post-Incident Activity

The recommended and required activities of each phase are described herein.

**Figure 37: Centrally-Managed Policies and Procedures**



**Document Information**

Document Detail  
Edit History  
Support Documents  
Header / Footer

Generate  
Preview  
Reset: CP-GEN-5-0-XMLC

Version: 5.0  
Created: 06/11/2014 05:57:09 PM  
By: tpa\_hq

Save Close

**5.3 Recovery Declaration**

Upon successfully completing testing and validation, the <role name> will formally declare recovery efforts complete, and that (sn) is in normal operations. (sn) business and technical POCs will be notified of the declaration by the Contingency Plan Coordinator. The recovery declaration statement notifies the Contingency Plan Team and executive management that the (sn) has returned to normal operations.

**5.4 User Notification**

After the recovery declaration statement is made, notifications are sent to users and customers. Notifications to customers are made in accordance with predetermined notification procedures.

Tip:  
Instruction: Describe the notification procedures. Ensure that the procedures described are consistent with Service Level Agreements and contracts.

Remove this tip before submission.

**5.5 Cleanup**

Cleanup is the process of cleaning up or dismantling any temporary recovery locations, restocking supplies used, returning manuals or other documentation to their original locations, and readying the system for a possible future contingency event.

Tip:  
Instruction: Describe cleanup procedures and tasks including cleanup roles and responsibilities. Insert cleanup responsibilities in Table 5-1. Add additional rows as needed.

Remove this tip before submission.

**Table 5-1: Cleanup Roles and Responsibilities**

Role	Cleanup Responsibilities

**5.6 Returning Backup Media**

It is important that all backup and installation media used during recovery be returned to the offsite data storage location. The following procedures should be followed to return backup and installation media to its offsite data storage location.

Tip:  
Instruction: Provide procedures for returning retrieved backup or installation media to its offsite data storage location. This may include proper logging and packaging of backup and

**Figure 38: Built-in Content Authoring**

Compliance metrics for policies and procedures can also be tracked for the users and by policy/procedure to meet adherence requirement to specific regulation or standard.

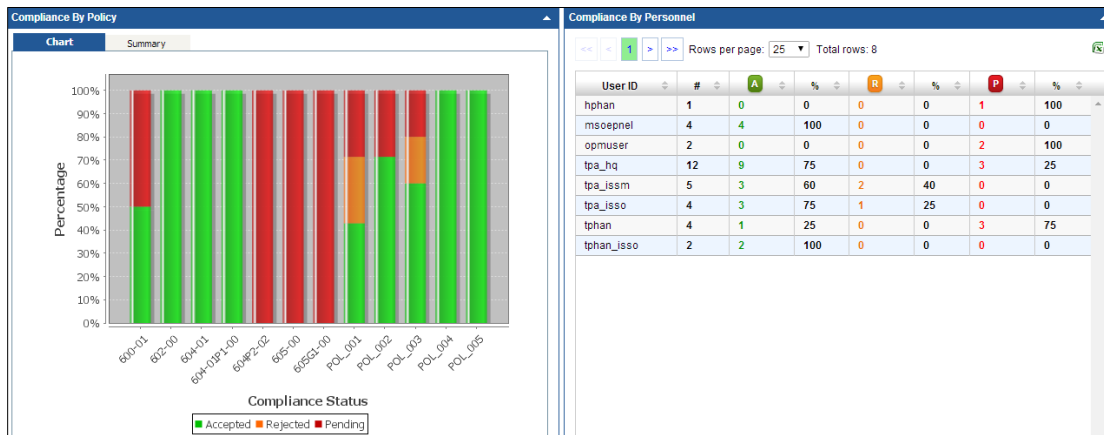


Figure 39: Policy Compliance

## 8 MONITOR Phase

Ongoing security reviews, assessments, and remediation of vulnerabilities and corrective actions are performed. Results of vulnerability assessments, independent audits, and continuous monitoring assessments are managed with risk management oversight performed by the organization. Corrective actions are remediated and updated by system owners.

Regulations or Standards	Requirements	
COBIT ISO 27001	A.10.1.2: Change management A.10.2.2: Monitoring and review of third party services A.10.2.3: Managing changes to third party services	MEA01: Monitor, Evaluate and Assess Performance and Conformance MEA02: Monitor, evaluate and assess the system of internal control MEA03: Monitor, evaluate and assess compliance with external requirements.
ARS FEDRAMP FISMA MARS-E	CA-7: Continuous Monitoring NIST 800-137 Information Security Continuous Monitoring FedRAMP Continuous Monitoring Strategy Guide	
HIPAA HITECH Meaningful Use	164.308(a)(1)(ii)(D): Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. → Have you implemented procedures to regularly review records of IS activity such as audit logs, access reports, and security incident tracking? 164.308(a)(8): Evaluation. Perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart. → Have you established a plan for periodic technical and non-technical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of EPHI, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart?	

Regulations or Standards	Requirements
NIST CSF	PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition. PR.DS-7: Unnecessary assets are eliminated. DE.CM-1: The network is monitored to detect potential cybersecurity events. DE.CM-8: Vulnerability assessments are performed. DE.DP-5: Detection processes are continuously improved.
NERC CIP	CIP-007 R4: Security Event Monitoring
PCI DSS	12.5.2: Monitor and analyze security alerts and information, and distribute to appropriate personnel. 12.10.5: Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems.  <i>Best Practices – 1. Monitoring of security controls - such as firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), file-integrity monitoring (FIM), anti-virus, access controls, etc. - to ensure they are operating effectively and as intended.</i> <i>Best Practices – 5. Periodic reviews and communications should be performed to confirm that PCI DSS requirements continue to be in place and personnel are following secure processes. These periodic reviews should cover all facilities and locations, including retail outlets, data centers, etc., and include reviewing system components (or samples of system components), to verify that PCI DSS requirements continue to be in place—for example, configuration standards have been applied, patches and AV are up to date, audit logs are being reviewed, and so on. The frequency of periodic reviews should be determined by the entity as appropriate for the size and complexity of their environment.</i>
SANS Critical Security Controls	CSC-4: Continuous Vulnerability Assessment and Remediation

In addition to TrustedAgent's support of vulnerability assessment scanners TrustedAgent's continuous monitoring wizard enables the organization to define and select key controls to be retested on annual basis as mandated by organization-wide ongoing compliance (e.g., annual assessment controls), continuously over a three-year cycle (e.g., three subsets of controls for FISMA continuous security authorization), or due to replacement of the asset or the asset's configuration, or completion of remediation.

**Continuous Monitoring Wizard**

**Control Filters**

☒ Include Inherited Controls

☒ Include Controls accepted as Risk Based Decisions

☒ Include Controls other than documented in Place

**Control Selection**

Component:

Subcomponent:

Type:

Entity:

[Refresh Controls](#)

**Add Controls**

Template Name:

Family:

Control:

Note: Radio buttons at the family level will be displayed as blank when their selection state does not apply to all of the controls in that family. Please expand the family to view individual selection states of each control.

Family	Control Title	Volatile					2012					2013					2014					2015					Control Selection Source			
		Yes	No	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No	Year 1	Year 2	Year 3										
Access Control		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>				<a href="#">Delete</a>										
Asset Management	ID-AM-1 Device and System Inventory	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	AA	AA	AA	<a href="#">Delete</a>										
	ID-AM-2 Software Platform and Application Inventory	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	AA	AA	AA	<a href="#">Delete</a>										
	ID-AM-4 External Information System Services	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	AA	AA	AA	<a href="#">Delete</a>										
	ID-AM-5 Prioritization of Resources	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	AA	AA	AA	<a href="#">Delete</a>										
	ID-AM-6 Roles and Responsibilities of Workforce and Third-Party Stakeholders	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	AA	AA	AA	<a href="#">Delete</a>										
Governance		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>				<a href="#">Delete</a>										
Maintenance		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>				<a href="#">Delete</a>										

Figure 40: Continuous Monitoring Wizard

## Financial Justification Model for TrustedAgent GRC

In this part of our whitepaper, we propose a quantitative technique to provide measureable and cost justification to senior management to support the acquisition of TrustedAgent to replace manual methods supporting security authorization. Consider the following scenario in the justification:

An organization with requires an enterprise deployment of TrustedAgent to manage security authorization across for 30 systems of Moderate level. The organization intends to host TrustedAgent in its data center using acquired hardware and software with rooms to support future growth. In the example, the proposed organization licenses TrustedAgent as an enterprise tool, therefore enables the organization to support up to 100 entities across all organization-wide programs.

FINANCIAL MODEL FOR JUSTIFICATION OF TRUSTEDAGENT GRC						
Year	1	2	3	4	5	
Hardware (based on large deployment requirements)	\$ 50,000					
Software (based on large deployment requirements)	\$ 50,000					
TrustedAgent enterprise software licensing	\$ 105,000					
Recurring maintenance (estimated at 25% of total software/hardware cost)		\$ 51,250	\$ 51,250	\$ 51,250	\$ 51,250	
Recurring professional services		\$ 10,000	\$ 10,000	\$ 10,000	\$ 10,000	
Initial implementation professional services	\$ 5,000					
Training	\$ 5,000					
Total Costs	\$ 215,000	\$ 61,250	\$ 61,250	\$ 61,250	\$ 61,250	

**Figure 41: Financial Model for TrustedAgent GRC**

The initial software and hardware investment is based on a large enterprise deployment consisting of an application server and a backend database server. The servers are Windows-based with Tomcat and Oracle or SQL Server. Both servers can be virtualized, but must be physically on separate hardware. The model also assumes no legacy data to migrate and using NIST 800-53 controls. Professional services are limited to installing TrustedAgent application and conduct training to the organization.

Using the metrics discussed from the ISACA study<sup>1</sup> and those gathered by Trusted Integration, it is then possible to derive cost savings vs. manual methods for the activities using TrustedAgent. The savings are annualized similar to the initial investment and recurring expenses by the organization.

	Year	1	2	3	4	5
<b>Cost savings elements</b>						
Content management			\$ 9,303	\$ 9,303	\$ 9,303	\$ 9,303
Inventory and Asset Management			\$ 4,902	\$ 4,902	\$ 4,902	\$ 4,902
Security categorization						
Baseline control selection			\$ 46,587			
Common Controls			\$ 16,540	\$ 4,962	\$ 4,962	\$ 4,962
Control implementation			\$ 39,721	\$ 39,721	\$ 39,721	\$ 39,721
Control assessment			\$ 57,375	\$ 57,375	\$ 57,375	\$ 57,375
Aggregated (average) FTE reduction (as indicated below):			\$ 136,125			
Finding and weakness management						
Performance metrics and management dashboard						
Regulatory document reporting						
Continuous monitoring						
<b>Total Values</b>		<b>\$ -</b>	<b>\$ 310,553</b>	<b>\$ 116,264</b>	<b>\$ 116,264</b>	<b>\$ 116,264</b>

**Figure 42: Values Generated by TrustedAgent GRC vs. Manual Methods**

<sup>1</sup> "A framework for Estimating ROI of Automated Internal Controls", ISACA, 2011

"Cost of Compliance Survey 2013", Thomson Reuters, 2013

"TrustedAgent Benchmarking – TrustedAgent and Security Authorization White Paper", Trusted Integration, 2013



Once the savings are determined, annual cash flows and cumulative cash flows can be calculated leading to the determination of internal rates of return (IRR) and breakeven period for the organization.

Year	1	2	3	4	5
Annual Cash flow	\$ (215,000)	\$ 249,303	\$ 55,014	\$ 55,014	\$ 55,014
Cumulative Cash flow	\$ (215,000)	\$ 34,303	\$ 89,317	\$ 144,330	\$ 199,344
IRR - 5 YR	51%				
IRR - 4 YR (full SA cycle after tool acquisition)	46%				
IRR - 3 YR	35%				
Breakeven Period in Months	22				

**Figure 43: Internal Rates of Return of Investment in TrustedAgent GRC**

The results demonstrated in the above model are consistent in IRRs and breakeven noted in other studies including the one quoted in this paper. If the number of security authorization is greater than 30 entities, the IRR would be even more favorable for the organization, and the breakeven period would reduce accordingly due to the greater cost savings generated in manual work reduction.

## Conclusion

While authorization process can be complex and time-consuming, the highly scalable and customizable TrustedAgent GRC offers the optimal automated solution for any organization seeking a balance of between cost, expected requirements, and implementation time to meet the requirements to one or more regulatory frameworks or standards across multiple industries. The tool is also flexible and may be customized to incorporate organization-unique attributes or requirements. As the results, TrustedAgent seamlessly integrates into and enhances business processes for many organizations of different levels of cybersecurity or compliance maturity.

Using the outlined measures and requirements, organizations can present plausible and quantifiable business cases to support the acquisition of the GRC solution. Just as equally as important as having tangible justifications, organizations must not forget, that due to the complexity of GRC processes and the broad scope of applicability, not all justifications can be measured in dollars and cents. Organizations must also consider the intangibles including:

- Integration of key GRC process under one centralized risk management framework, allowing the organization to manage compliance and risk activities under one comprehensive, standardized, and enterprise-wide risk management (ERM) approach.
- Elimination of information silos and duplications of compliance activities.
- Gain visibility and timely access to information to support clear, data-oriented risk-based decisions.
- Penalty and risk reduction from noncompliance to stakeholders

By adopting TrustedAgent GRC, organizations demonstrate discipline and controls of key risk management processes to key internal and external stakeholders, as well as regulatory and industry-audit personnel. Opportunities to streamlining business and compliance operations and activities to produce time and cost savings are also gained. Organizations obtain greater peer and customer recognitions, and opportunities to command higher premium for the organizations' product and services.

Trusted Integration is a leading provider of Governance, Risk and Compliance (GRC) management solutions for government and commercial organizations. TrustedAgent is an adaptive, scalable GRC solution for organizations to standardize business processes, reduce complexities, and lower costs in the management, analysis, and remediation of risks across the enterprise to meet the challenging, complex, and ever-changing requirements of NIST Cybersecurity Framework, PCI, SOX, HIPAA, NERC, ISO, COBIT, FISMA, and many others.

TrustedAgent provides an unparalleled and cost-effective enterprise solution that enables organizations to inventory, assess, remediate, and manage risks and regulatory requirements before detrimental loss are sustained by the organization.



**Trusted Integration, Inc.**  
**525 Wythe Street**  
**Alexandria, VA 22314**  
**703-299-9171 Main**  
**703-299-9172 Fax**  
**[www.trustedintegration.com](http://www.trustedintegration.com)**