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.

Trusted Integration, Inc.
525 Wythe Street
Alexandria, VA 22314
www.trustedintegration.com

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: • Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.), • Identifies critical assets, threats, and vulnerabilities, and • Results in a formal risk assessment. 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.	
Note: → 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.

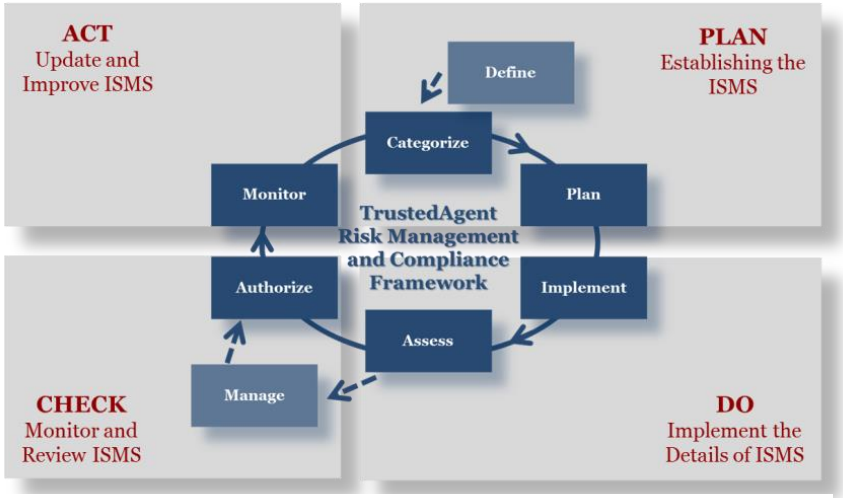


Figure 2: ISO 27001 vs. TrustedAgent Risk Management and Compliance Framework

1 DEFINE Phase

The Define Phase discusses requirements of having in place a formal risk management approach and the supporting policies and procedures. Under the selected risk management framework, a current list of inventory of IT and privacy systems, programs, critical assets, or vendors along with key attributes (ownership, purpose, key contacts, 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.

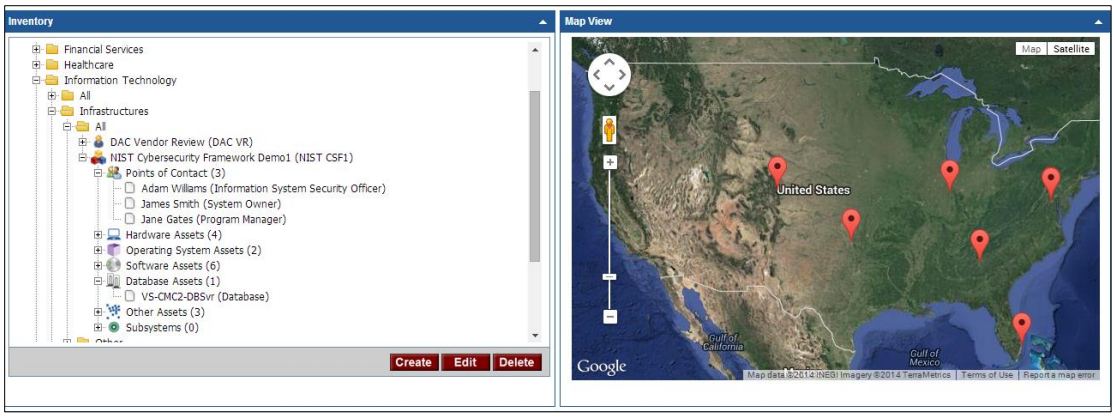
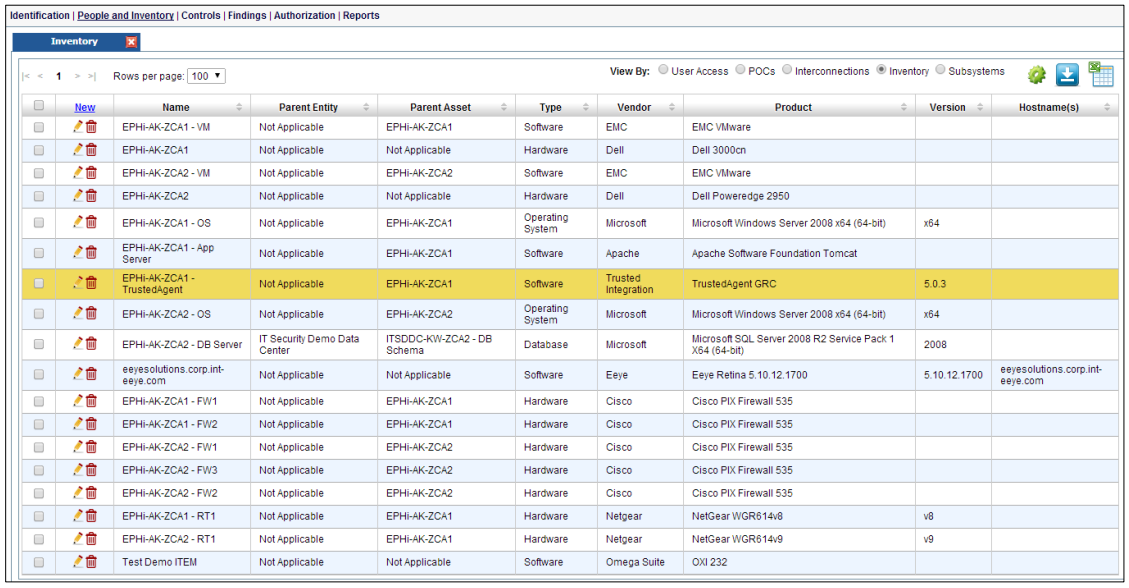


Figure 3: Inventory of Entities



New	Name	Parent Entity	Parent Asset	Type	Vendor	Product	Version	Hostname(s)
	EPHi-AK-ZCA1 - VM	Not Applicable	EPHi-AK-ZCA1	Software	EMC	EMC VMware		
	EPHi-AK-ZCA1	Not Applicable	Not Applicable	Hardware	Dell	Dell 3000cn		
	EPHi-AK-ZCA2 - VM	Not Applicable	EPHi-AK-ZCA2	Software	EMC	EMC VMware		
	EPHi-AK-ZCA2	Not Applicable	Not Applicable	Hardware	Dell	Dell Poweredge 2950		
	EPHi-AK-ZCA1 - OS	Not Applicable	EPHi-AK-ZCA1	Operating System	Microsoft	Microsoft Windows Server 2008 x64 (64-bit)	x64	
	EPHi-AK-ZCA1 - App Server	Not Applicable	EPHi-AK-ZCA1	Software	Apache	Apache Software Foundation Tomcat		
	EPHi-AK-ZCA1 - TrustedAgent	Not Applicable	EPHi-AK-ZCA1	Software	Trusted Integration	TrustedAgent GRC	5.0.3	
	EPHi-AK-ZCA2 - OS	Not Applicable	EPHi-AK-ZCA2	Operating System	Microsoft	Microsoft Windows Server 2008 x64 (64-bit)	x64	
	EPHi-AK-ZCA2 - DB Server	IT Security Demo Data Center	ITSDDC-KW-ZCA2 - DB Schema	Database	Microsoft	Microsoft SQL Server 2008 R2 Service Pack 1 X64 (64-bit)	2008	
	eeyesolutions.corp.int-eeye.com	Not Applicable	Not Applicable	Software	Eeye	Eeye Retina 5.10.12.1700	5.10.12.1700	eeyesolutions.corp.int-eeye.com
	EPHi-AK-ZCA1 - FW1	Not Applicable	EPHi-AK-ZCA1	Hardware	Cisco	Cisco PIX Firewall 535		
	EPHi-AK-ZCA1 - FW2	Not Applicable	EPHi-AK-ZCA1	Hardware	Cisco	Cisco PIX Firewall 535		
	EPHi-AK-ZCA2 - FW1	Not Applicable	EPHi-AK-ZCA2	Hardware	Cisco	Cisco PIX Firewall 535		
	EPHi-AK-ZCA2 - FW3	Not Applicable	EPHi-AK-ZCA2	Hardware	Cisco	Cisco PIX Firewall 535		
	EPHi-AK-ZCA2 - FW2	Not Applicable	EPHi-AK-ZCA2	Hardware	Cisco	Cisco PIX Firewall 535		
	EPHi-AK-ZCA1 - RT1	Not Applicable	EPHi-AK-ZCA1	Hardware	Netgear	NetGear WGR614v8	v8	
	EPHi-AK-ZCA2 - RT1	Not Applicable	EPHi-AK-ZCA1	Hardware	Netgear	NetGear WGR614v9	v9	
	Test Demo ITEM	Not Applicable	Not Applicable	Software	Omega Suite	OXI 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.

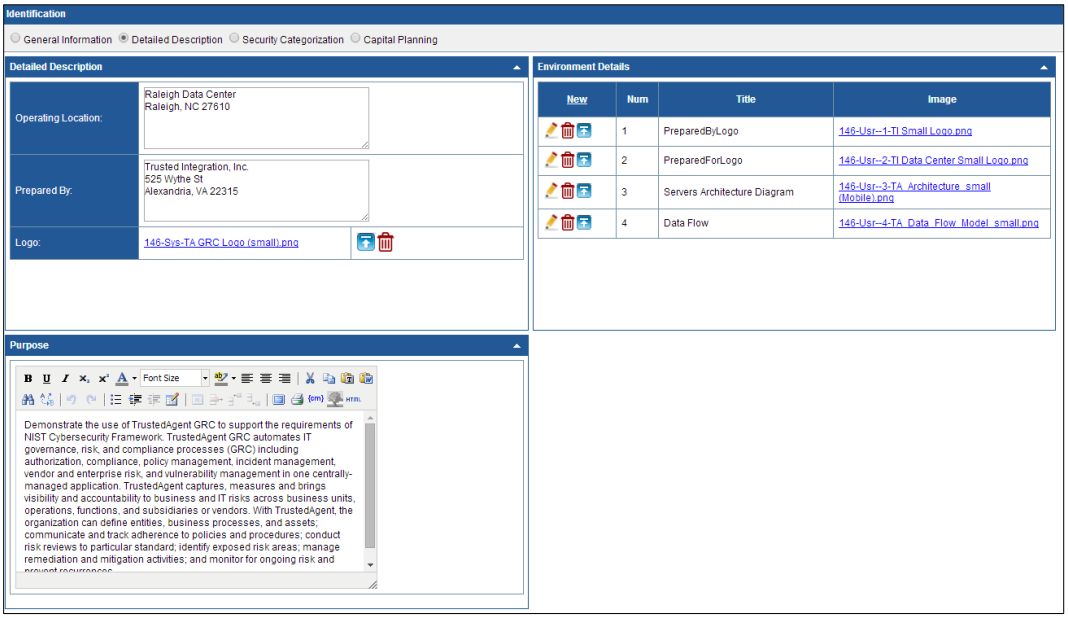


Figure 5: Repository of Reusable Key Diagrams

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.

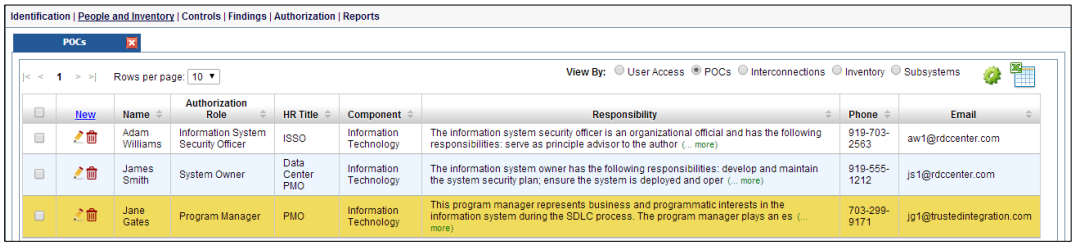


Figure 6: Key Contacts

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.

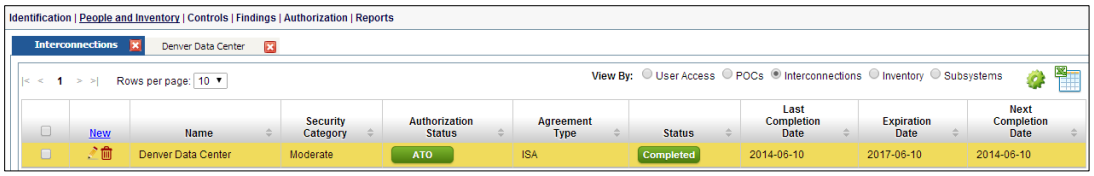


Figure 7: Interconnections

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.

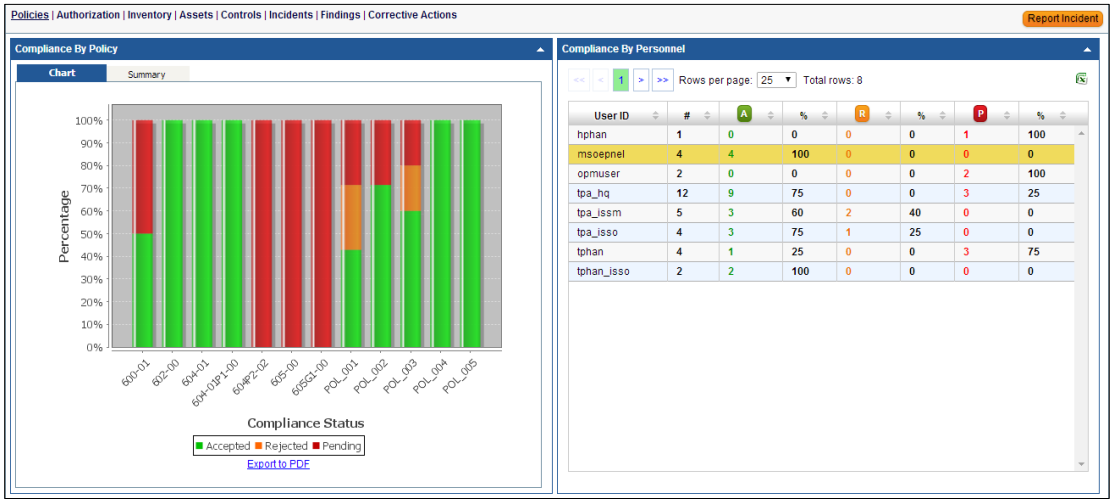


Figure 8: Policy Management

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	§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.) §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-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	*Recommended as best practices.*	
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.

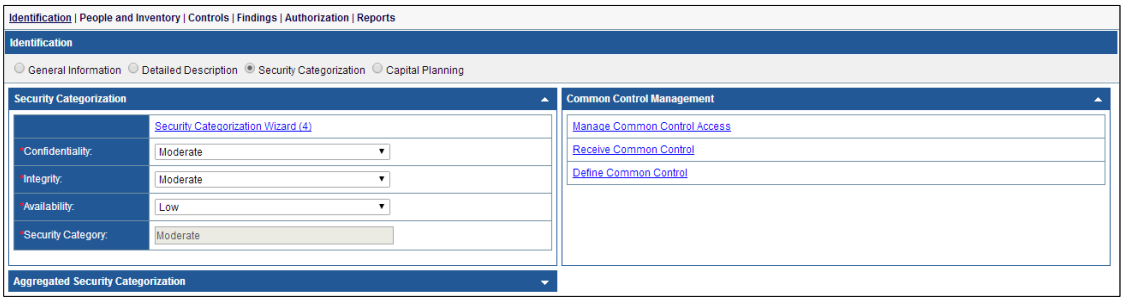
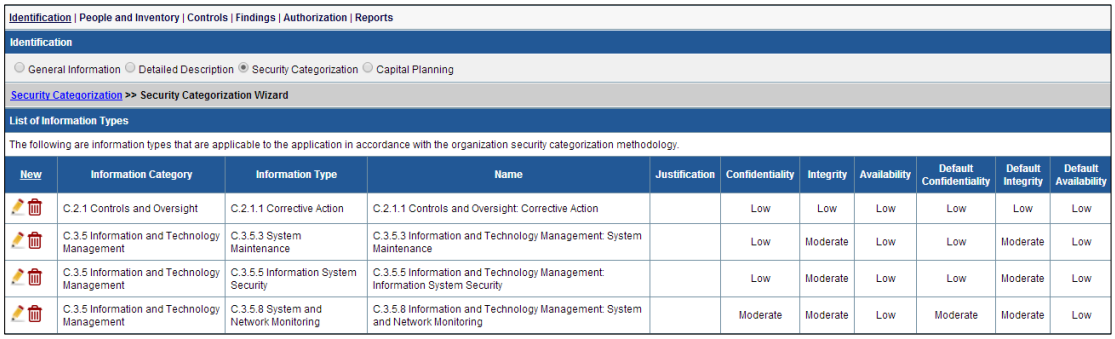


Figure 9: Security Categorization



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	*Recommended as best practices.*

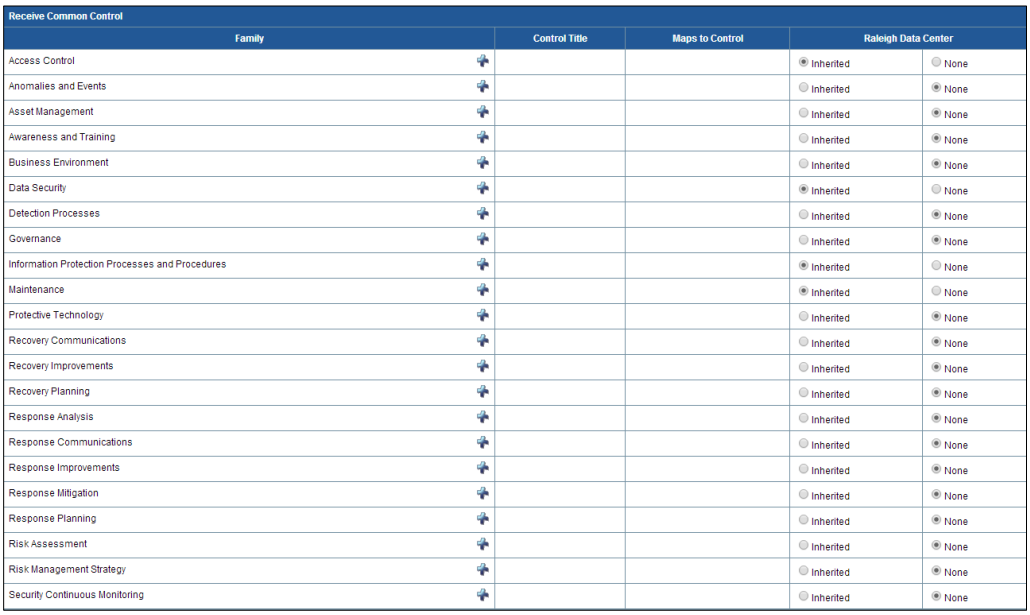


Figure 11: Receive Common Controls

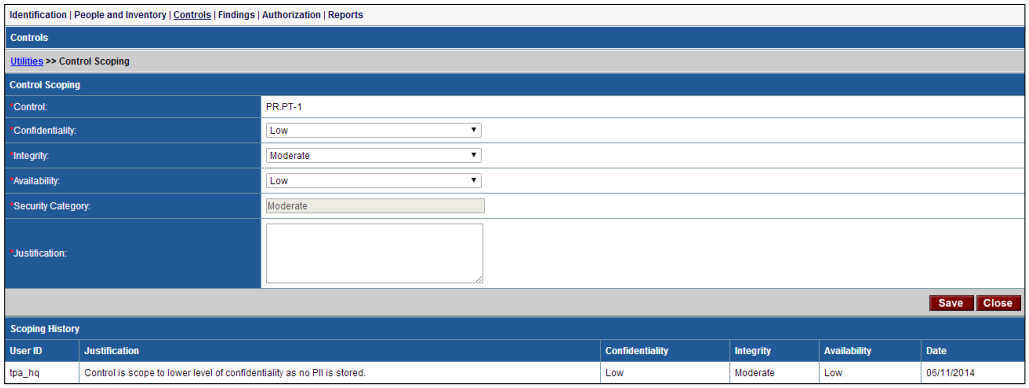


Figure 12: Control Scoping

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	☑	tpa_isso	12/11/2014
ID.AM-2 Software Platform and Application Inventory	☑	tpa_isso	12/11/2014
ID.AM-3 Organizational Interconnections and Data Flows	☑	tpa_isso	12/11/2014
ID.AM-4 External Information System Services	☑	tpa_isso	12/11/2014
ID.AM-5 Prioritization of Resources	☑	tpa_isso	12/11/2014
ID.AM-6 Roles and Responsibilities of Workforce and Third-Party Stakeholders	☑	tpa_isso	12/11/2014
ID.BE-1 Role of Organization and Supply Chain Protection	☐	tpa_isso	
ID.BE-2 Critical Infrastructure Plan	☐	tpa_isso	
ID.BE-3 Organizational Mission and Business Process Objectives	☐	tpa_isso	
ID.BE-4 Dependencies and Functions for Delivery of Critical Services	☐	tpa_isso	
ID.BE-5 Resilience and Delivery of Critical Services	☐	tpa_isso	
ID.GV-1 Security Policy and Procedures	☑	tpa_isso	12/11/2014
ID.GV-2 Information Security Roles and Responsibilities	☑	tpa_isso	12/11/2014
ID.GV-3 Cybersecurity Legal and Regulatory Requirements	☑	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	§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. §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. Meaningful Use Core Objective & 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.
NIST CSF	ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed. ID.GV-4: Governance and risk management processes address cybersecurity risks. ID.RM-2: Organizational risk tolerance is determined and clearly expressed ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis
NERC CIP	CIP-003: Security Management Controls
PCI DSS	*Best Practices - Business-as-Usual Processes.* 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: • 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). • 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). • Update PCI DSS scope and implement security controls as appropriate.
SANS Critical Security Controls	*Recommended as best practices.*

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.

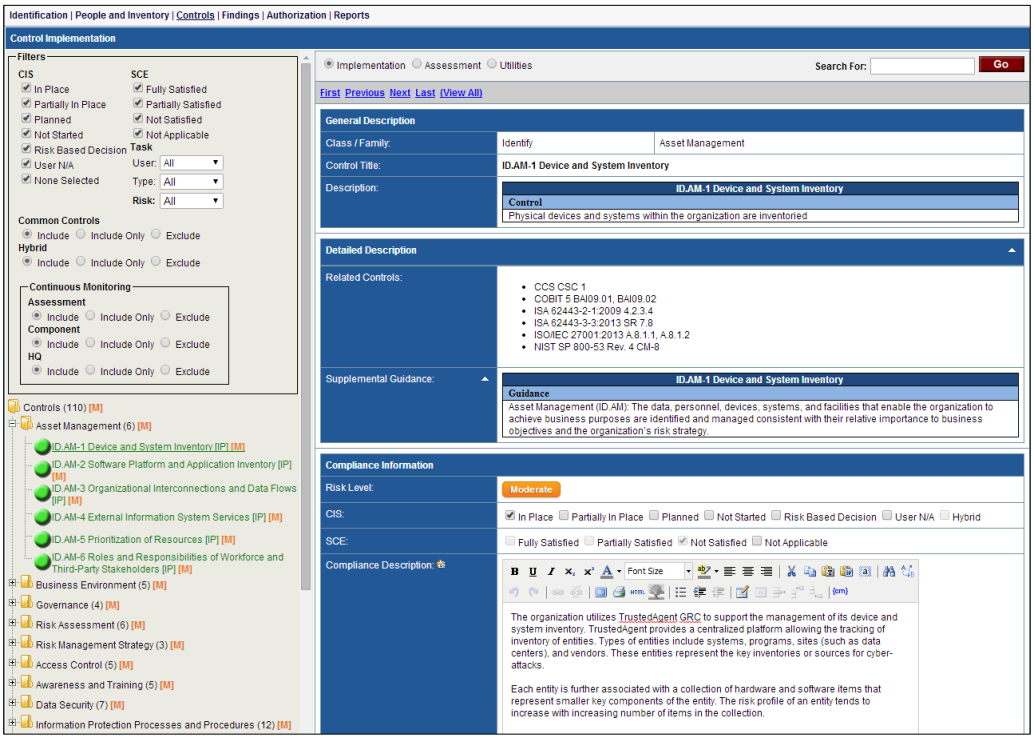


Figure 14: Control Implementation

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.

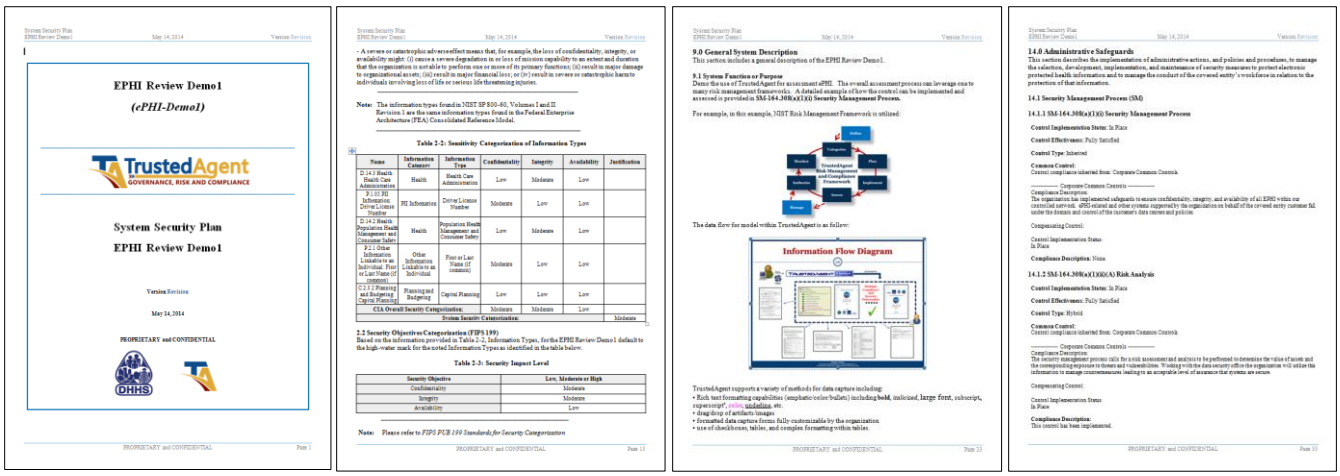


Figure 15: Automating System Security Plan

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.

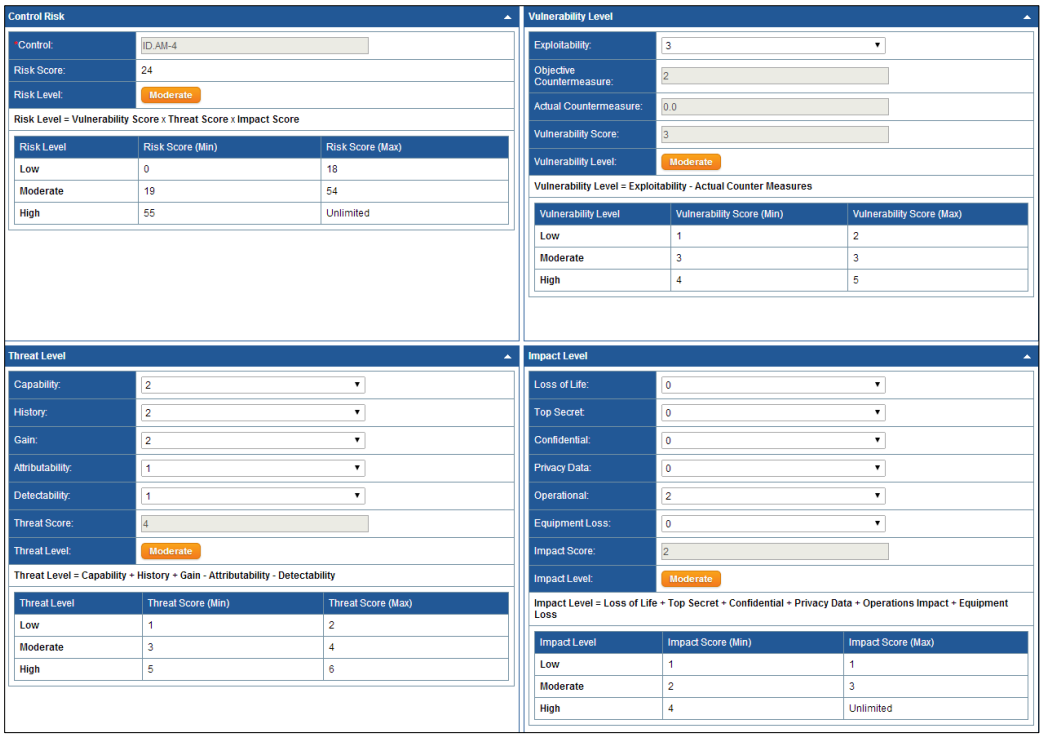


Figure 16: Control Risk Management

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: • Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.), • Identifies critical assets, threats, and vulnerabilities, and • Results in a formal risk assessment. 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	

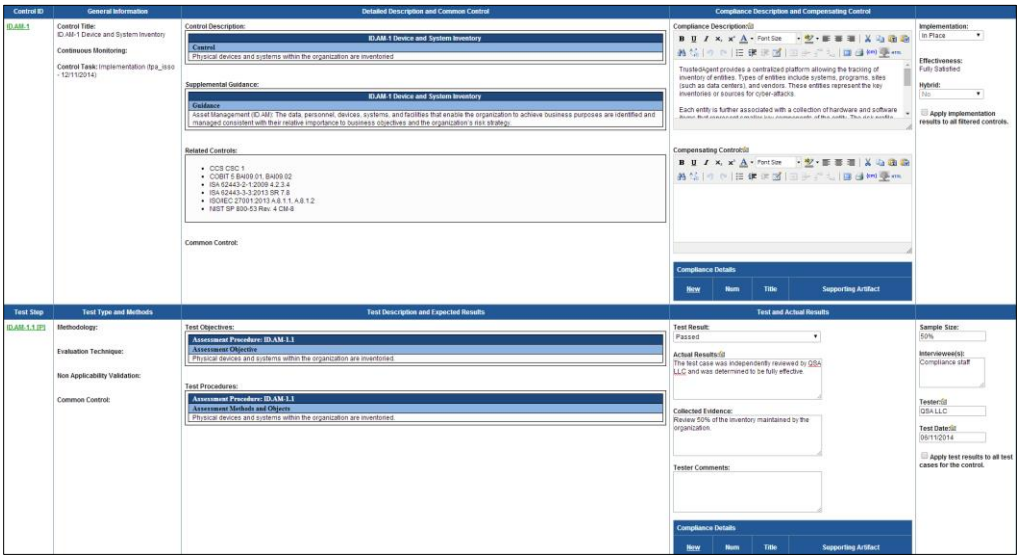


Figure 17: Control Assessment

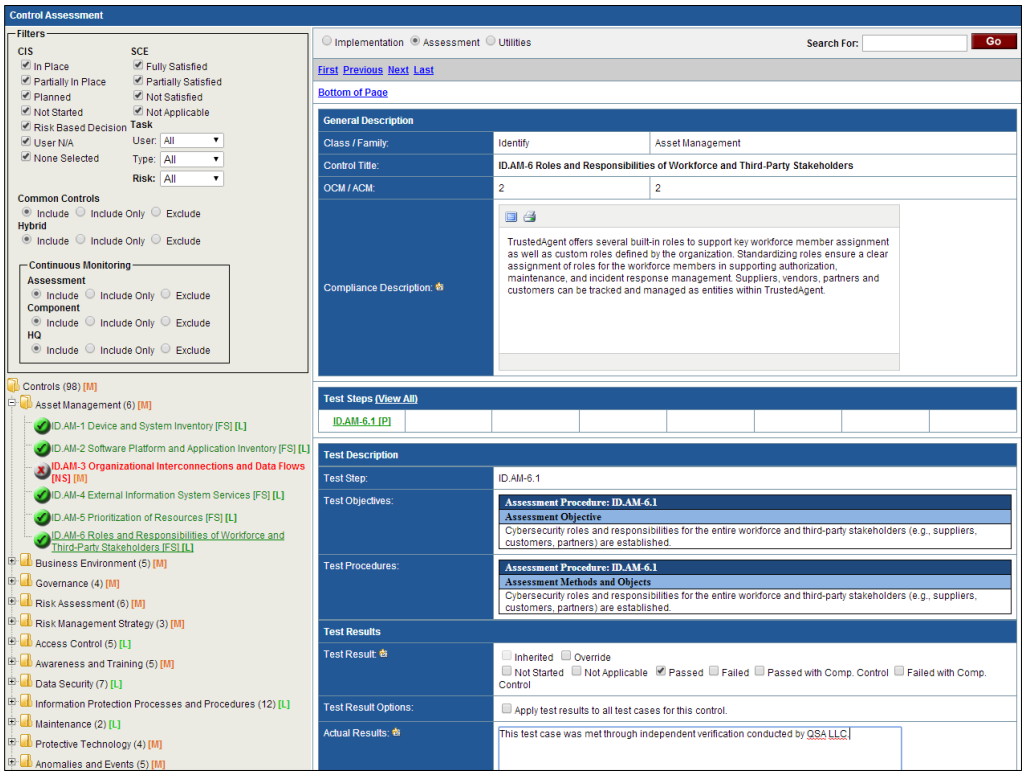


Figure 18: Control Assessment Details

TrustedAgent also offers integrated vulnerability assessment (VA) tools to schedule and conduct scans for supported vulnerability scanning applications (SAINT or OpenVAS). Where direct integration is not available, TrustedAgent supports vulnerability assessment imports in the form of the scanner's native XML output file. Additional scanners can be added through the addition of a XML connector (via configuration mapping file). Captured findings and vulnerabilities are visible through reports and on the organizational dashboard.

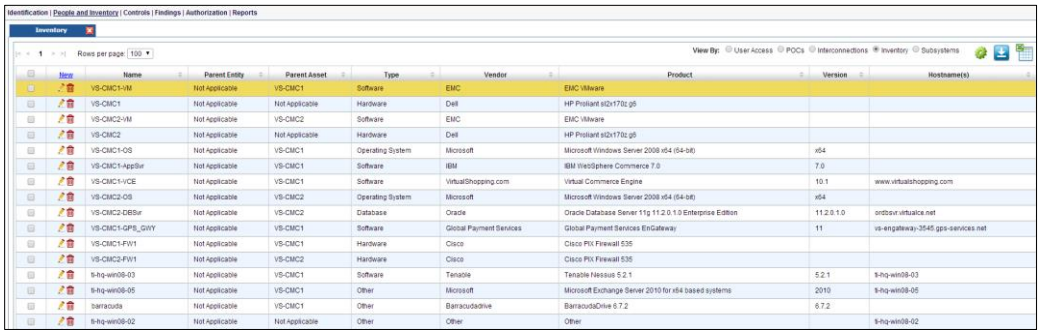


Figure 19: Asset Inventory

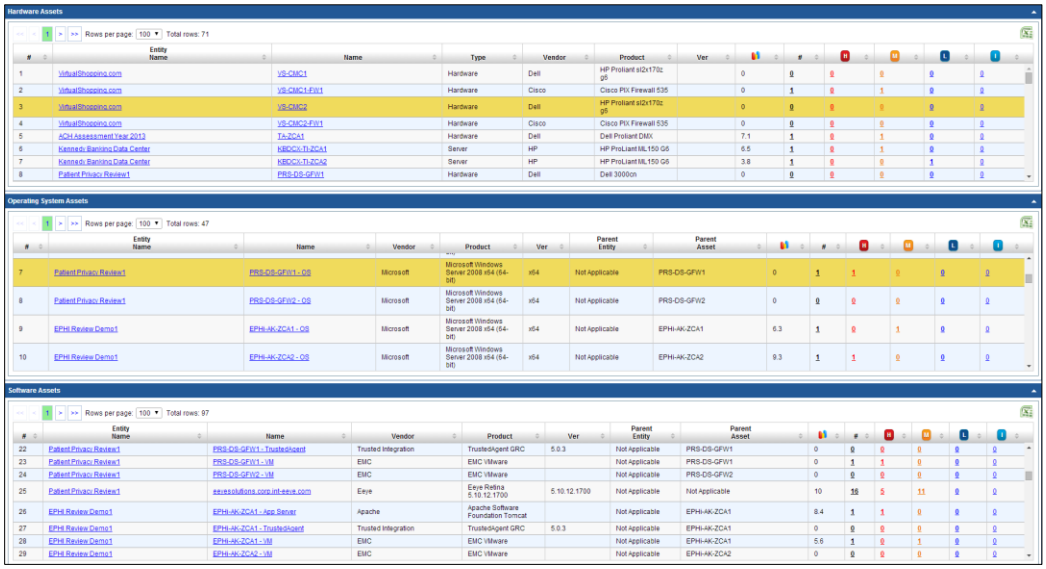


Figure 20: Vulnerabilities by Risk Level and Asset Group

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.

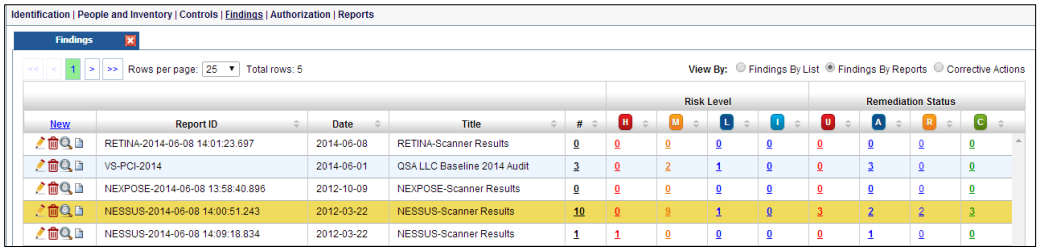
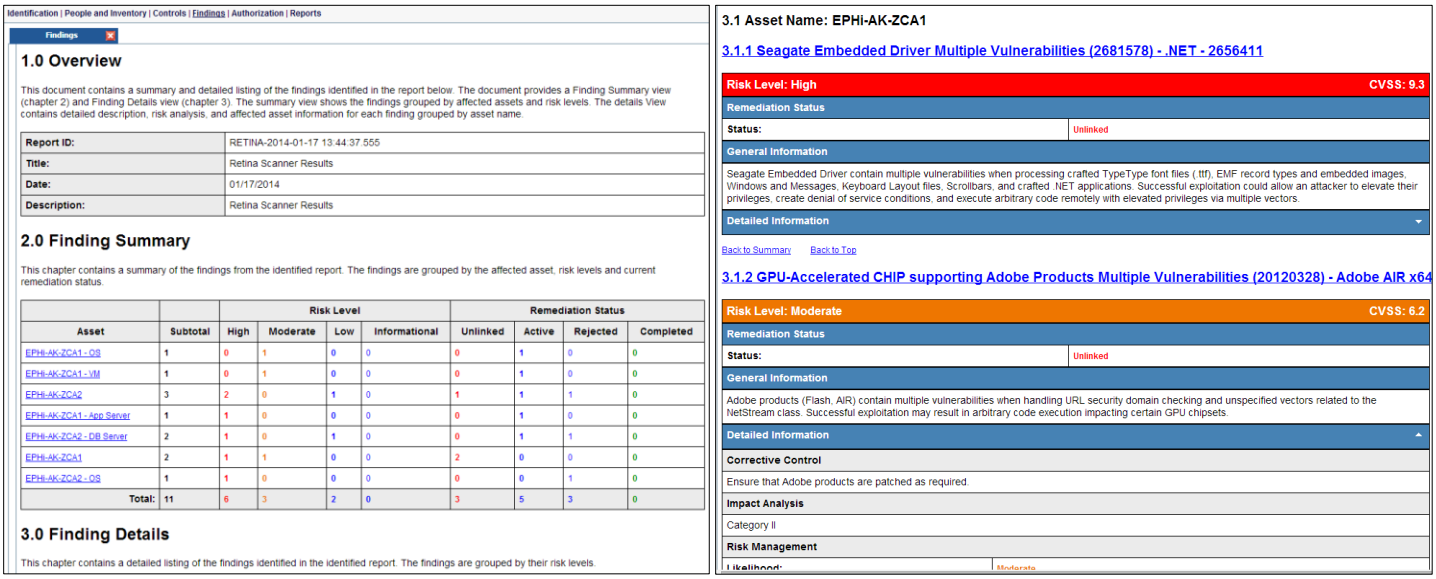


Figure 21: Finding Reports



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.

		Risk Level				Remediation Status			
Asset	Subtotal	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
Total:	11	6	3	2	0	3	5	3	0

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.

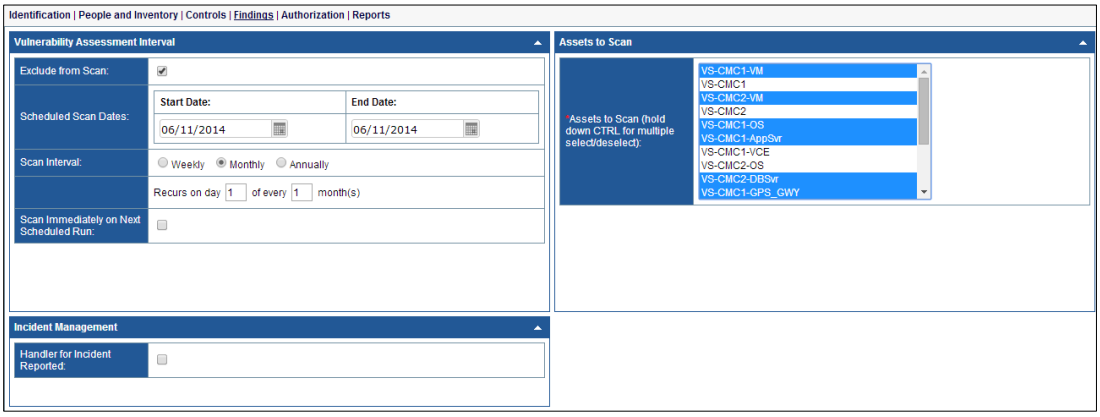
Impact Analysis

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

Recurs on day 1 of every 1 month(s)

Scan Immediately on Next Scheduled Run: ☐

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

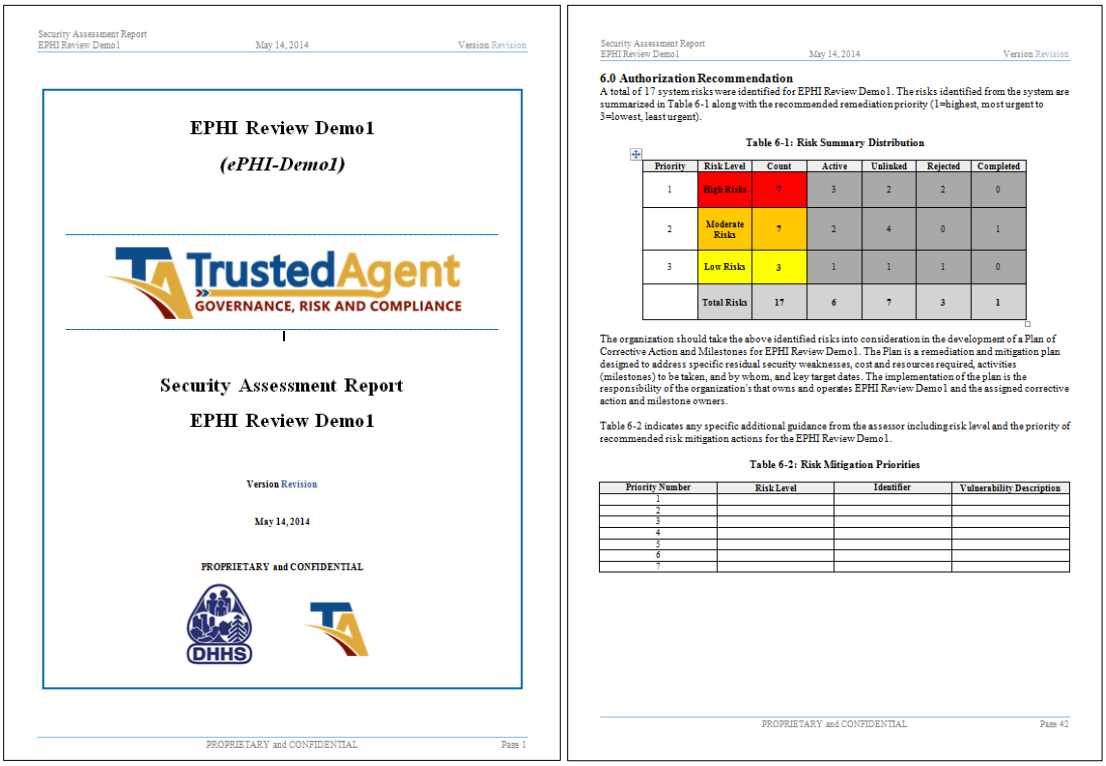
Incident Management

Handler for Incident Reported: ☐

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)

TrustedAgent
GOVERNANCE, RISK AND COMPLIANCE

Security Assessment Report

EPHI Review Demo1

Version Revision

May 14, 2014

PROPRIETARY and CONFIDENTIAL

DHHS

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
	Total Risks	17	6	7	3	1

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.	attNullByte (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.

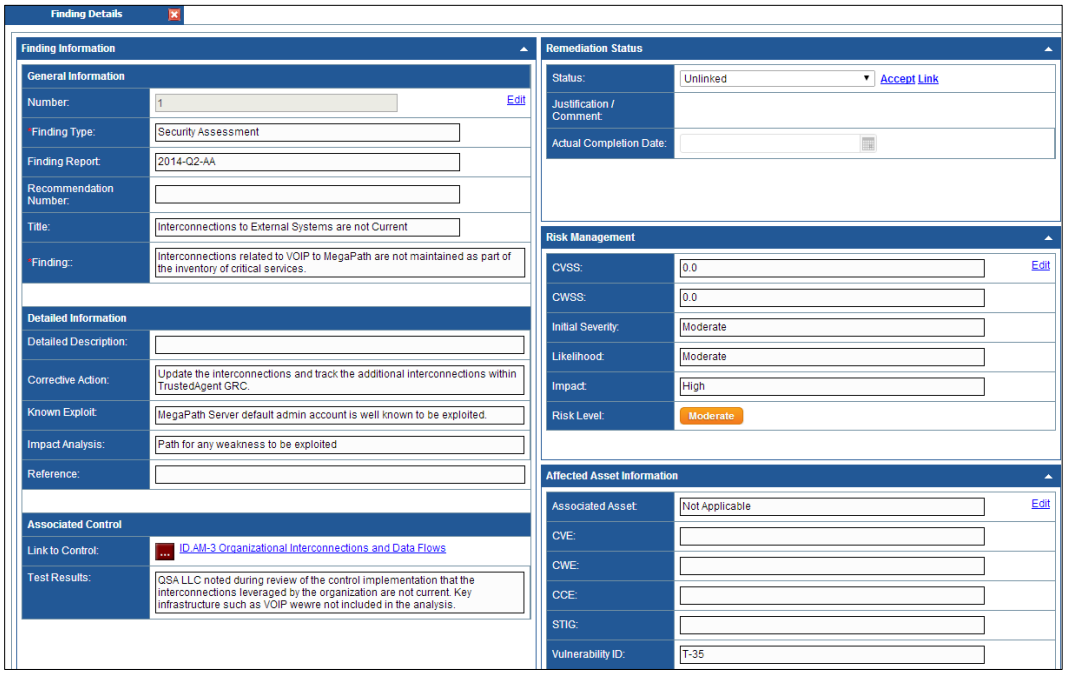


Figure 25: Finding Identification and Analysis

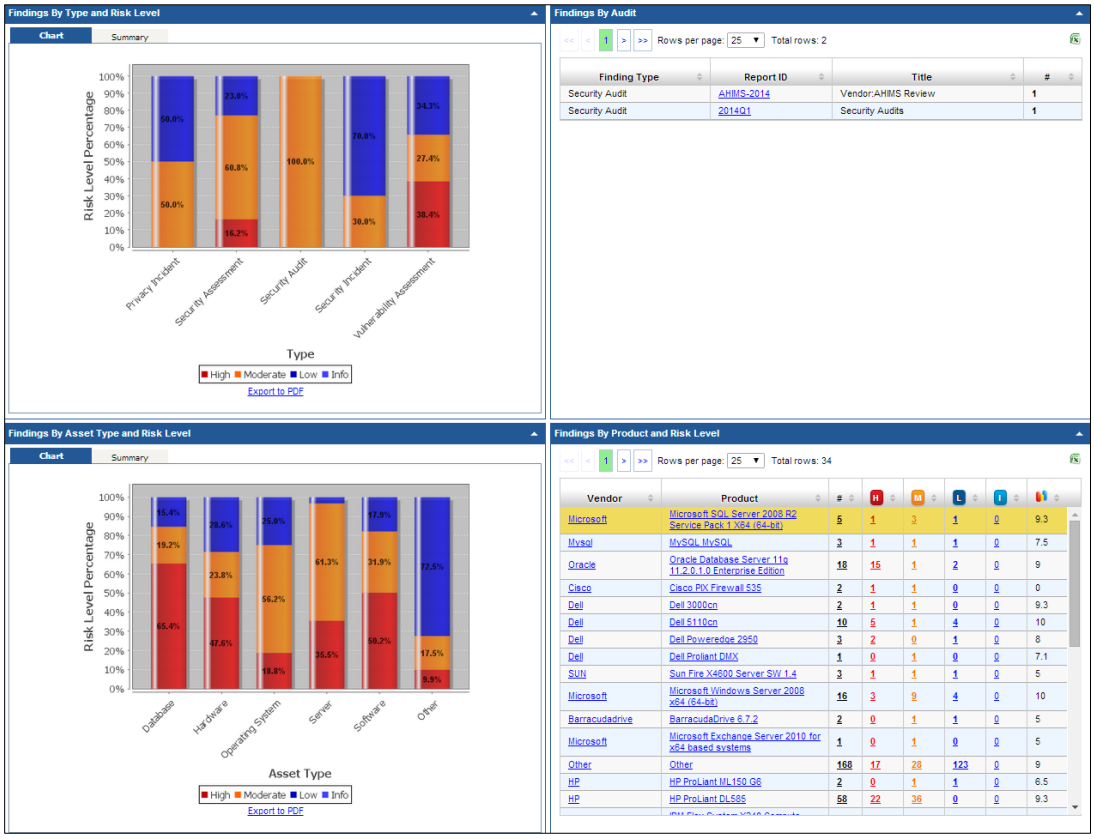


Figure 26: Findings by Type, Risk Level, and Product Group

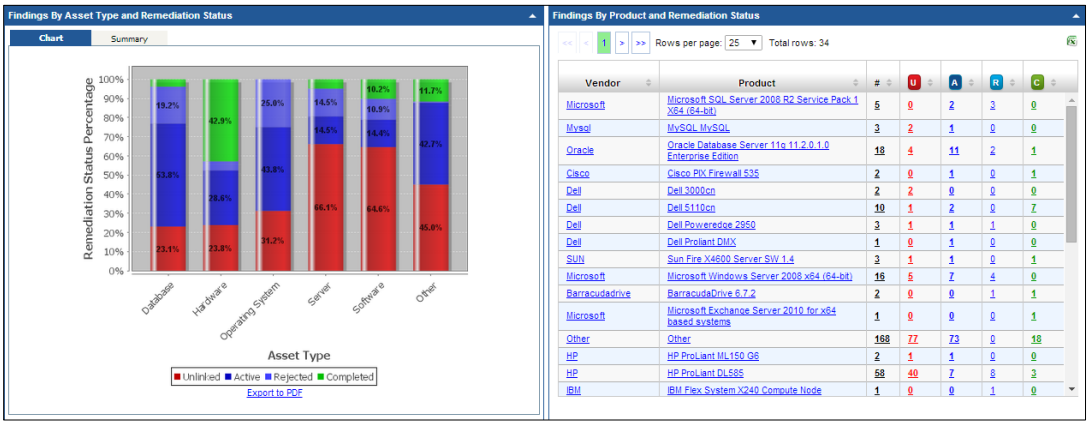


Figure 27: Findings by Remediation Status and Product Group

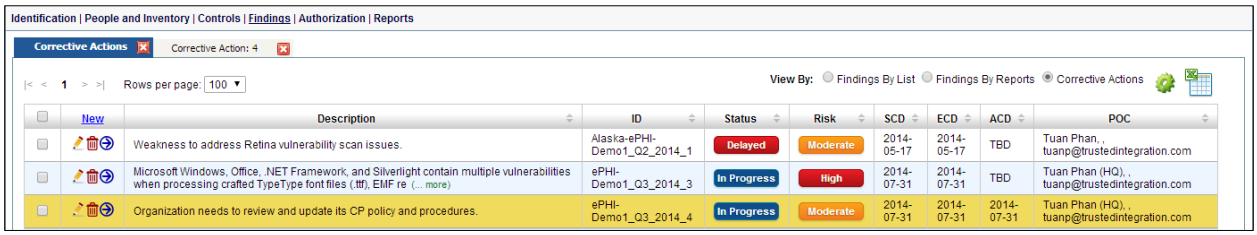


Figure 28: Corrective Action Summary

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: • R1: Cyber Security Incident Response Plan • R2: Implementation and testing of Cyber Security Incident Response Plans • R3: Cyber Security Incident Response Plan Review, Update and Communication
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.

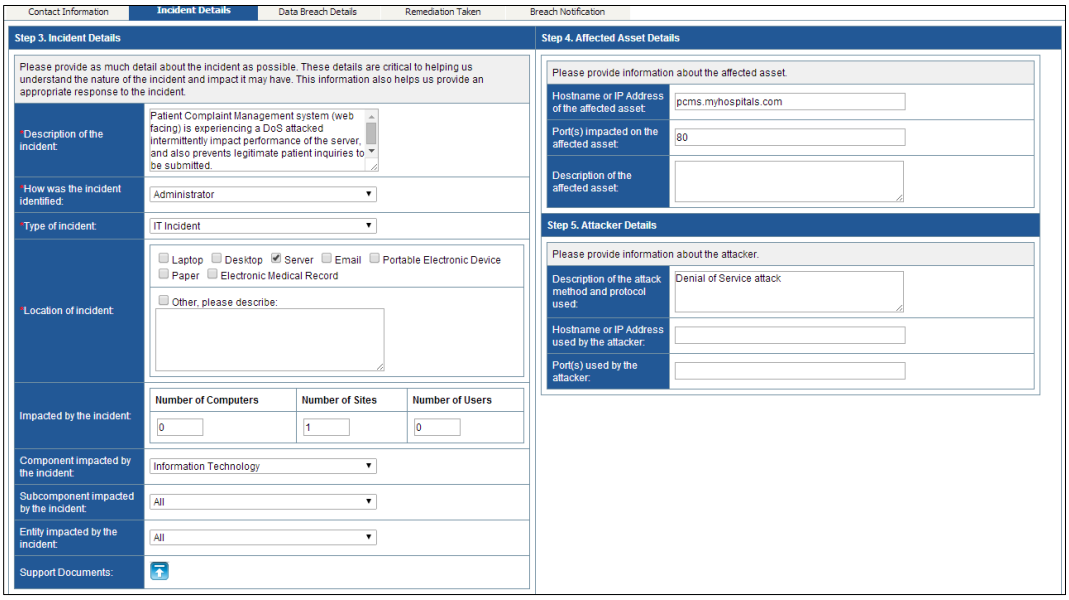
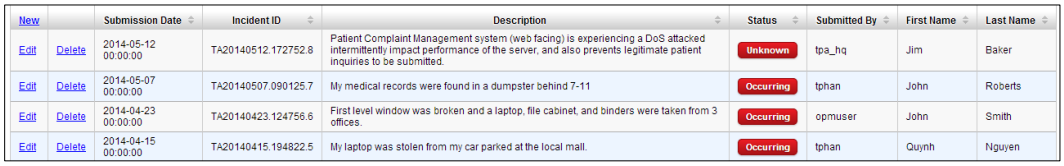


Figure 29: Incident Identification and Reporting



New		Submission Date	Incident ID	Description	Status	Submitted By	First Name	Last Name
Edit	Delete	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
Edit	Delete	2014-05-07 00:00:00	TA20140507.090125.7	My medical records were found in a dumpster behind 7-11	Occurring	tphan	John	Roberts
Edit	Delete	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
Edit	Delete	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

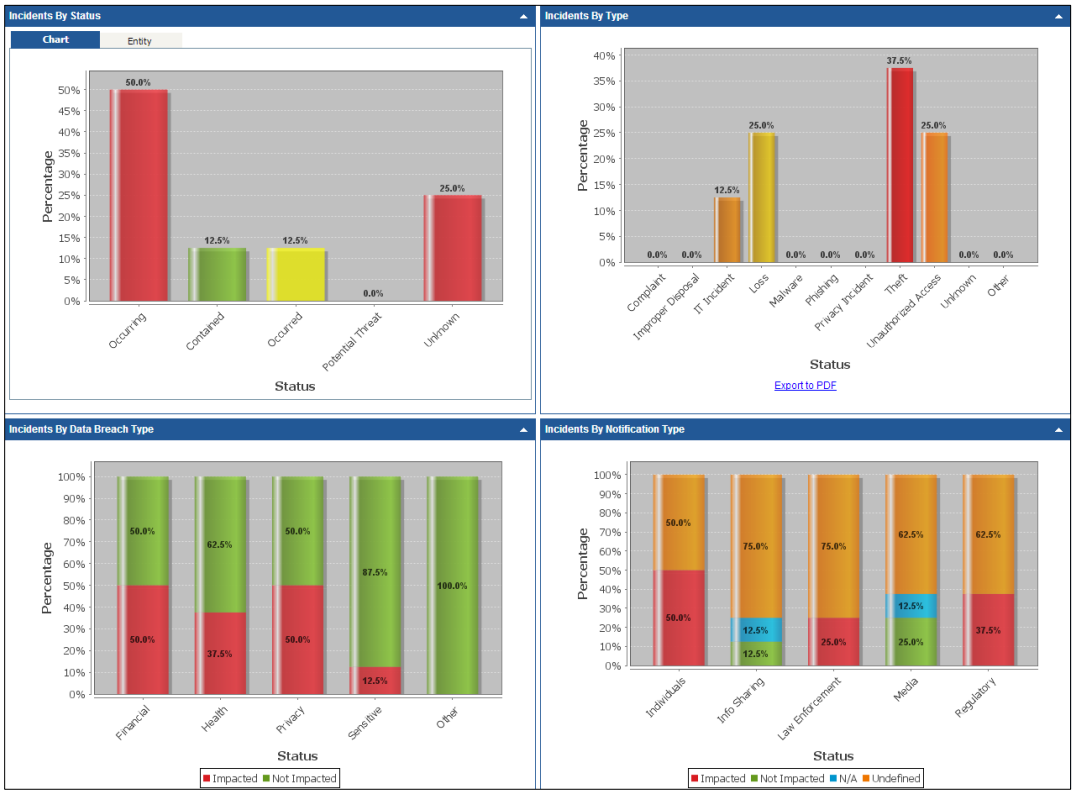


Figure 31: Incident Metrics

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.

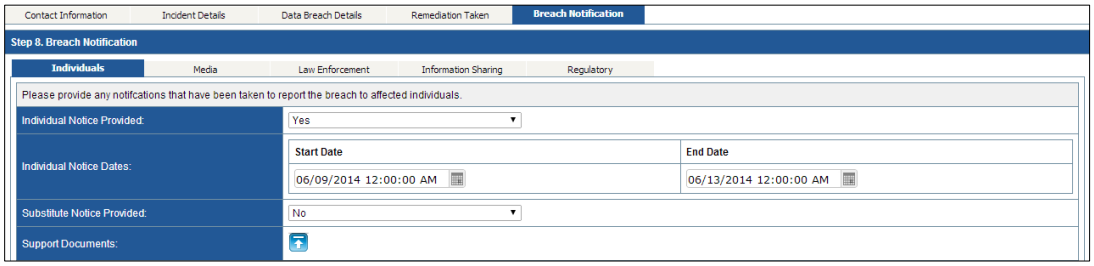


Figure 32: Incident Notifications

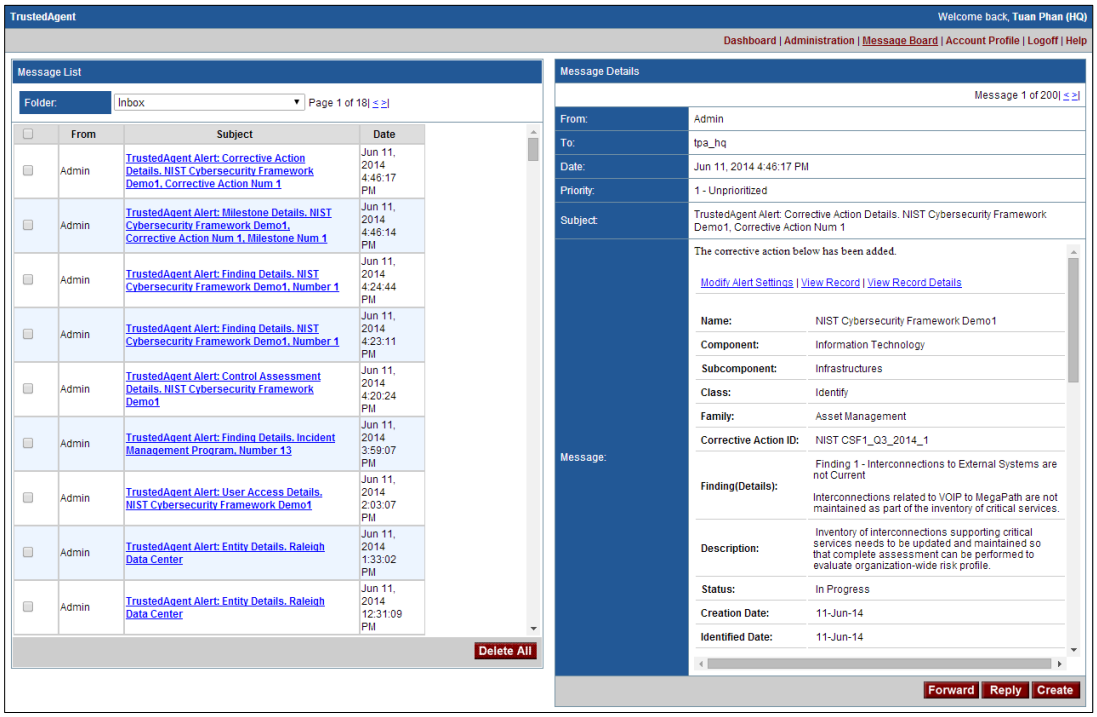


Figure 33: Message Board Notifications

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: • R1: Cyber Security Incident Response Plan • R2: Implementation and testing of Cyber Security Incident Response Plans • R3: Cyber Security Incident Response Plan Review, Update and Communication
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	*Recommended as best practices.*

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.

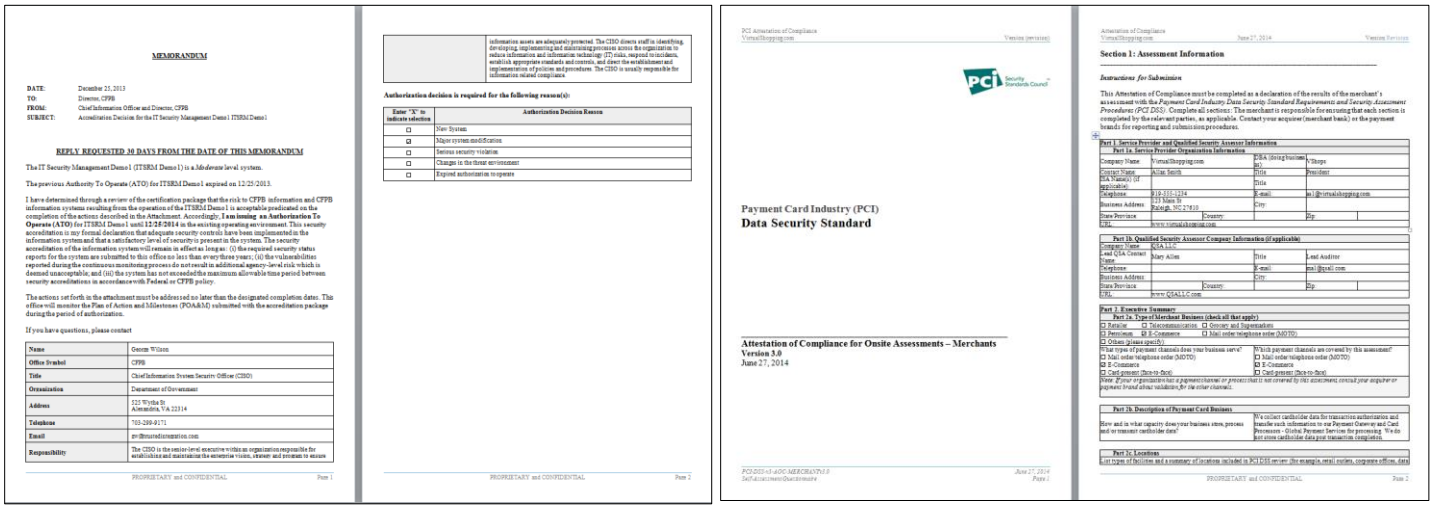


Figure 34: Sample ATO Letter / Attestation of Compliance for PCI DSS

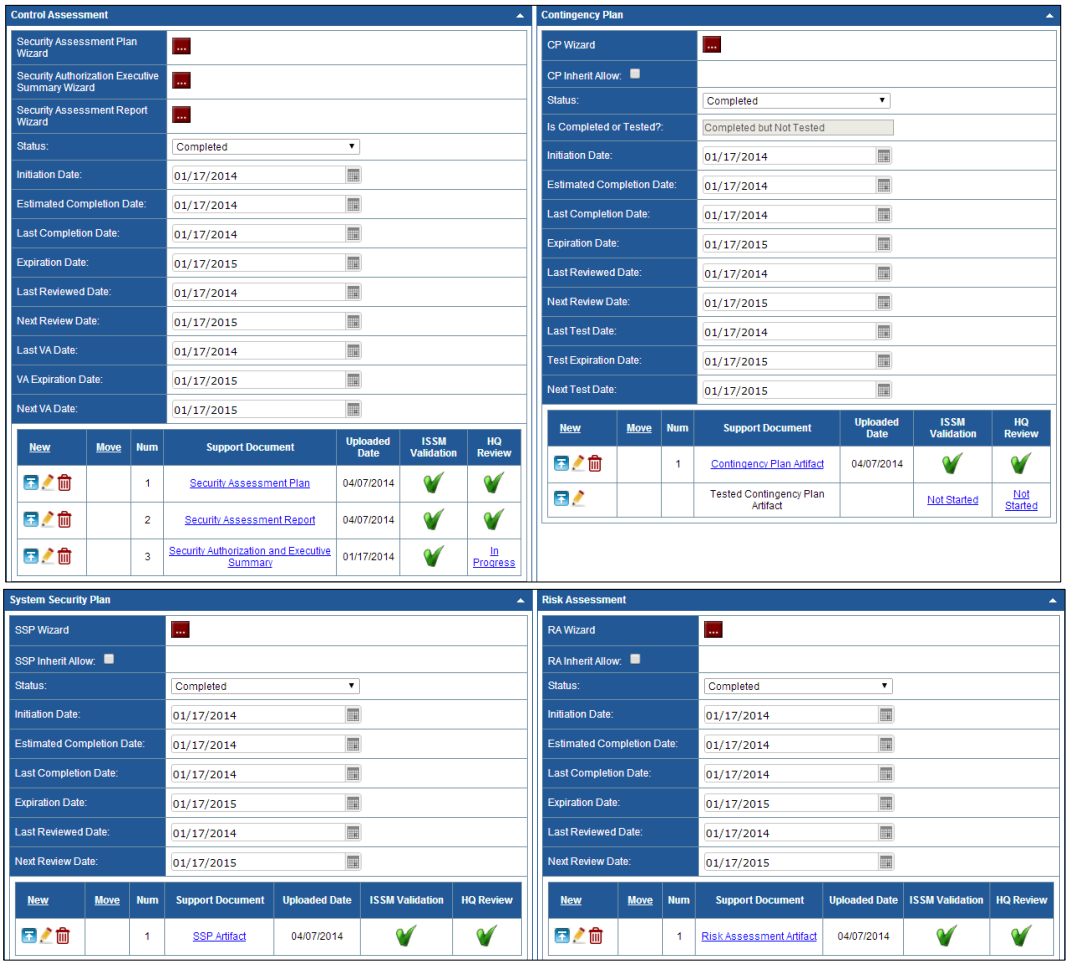


Figure 35: Tracking Key Performance Metrics of Regulatory Reports

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:

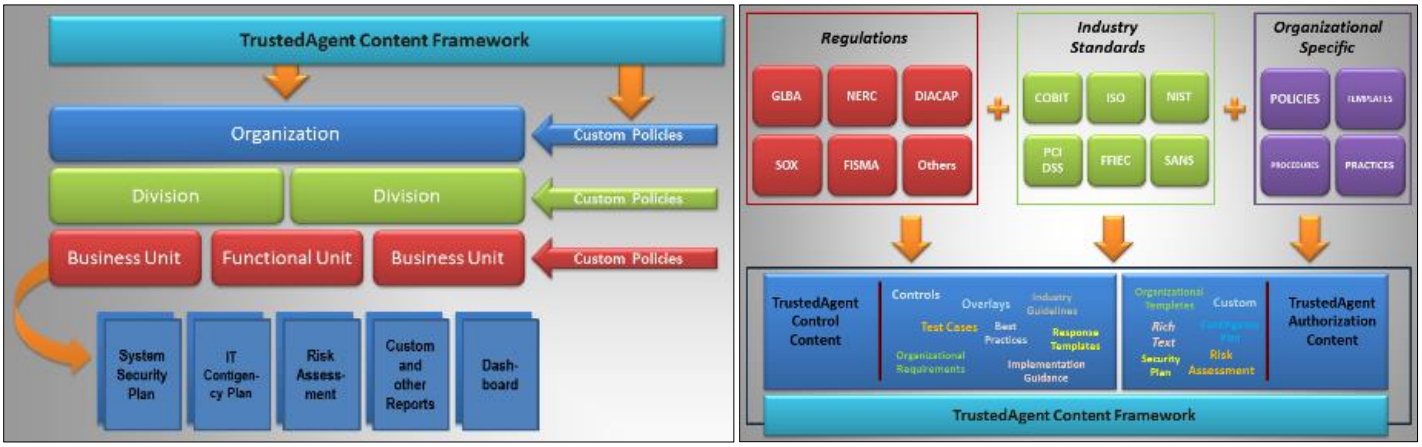


Figure 36: TrustedAgent Content Framework

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:

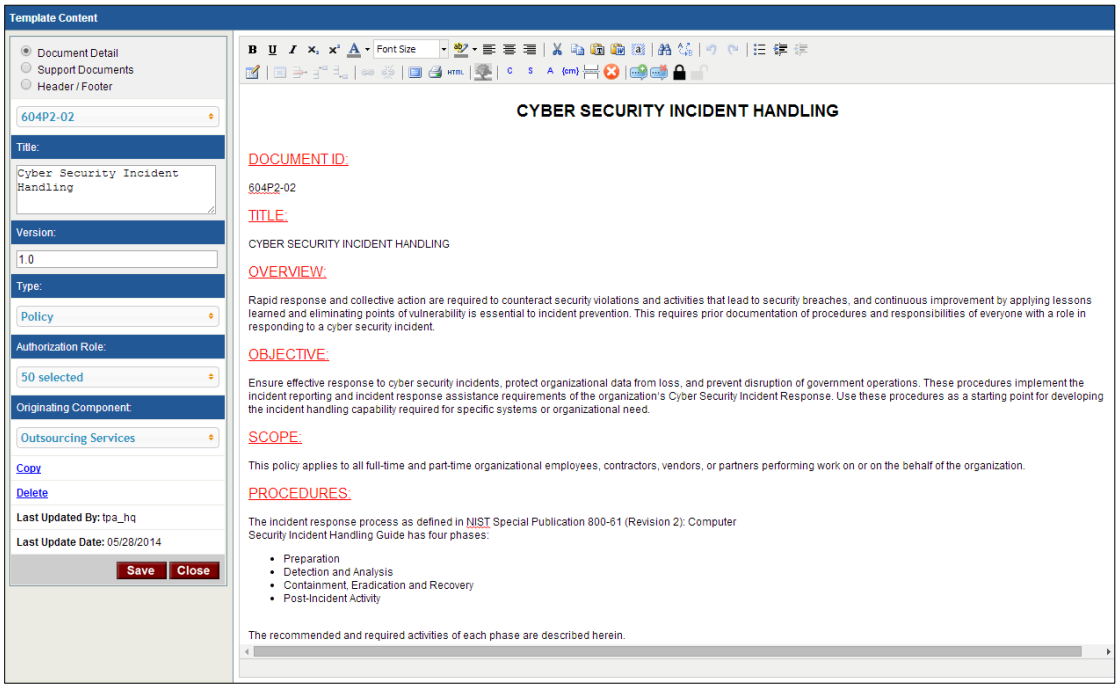


Figure 37: Centrally-Managed Policies and Procedures

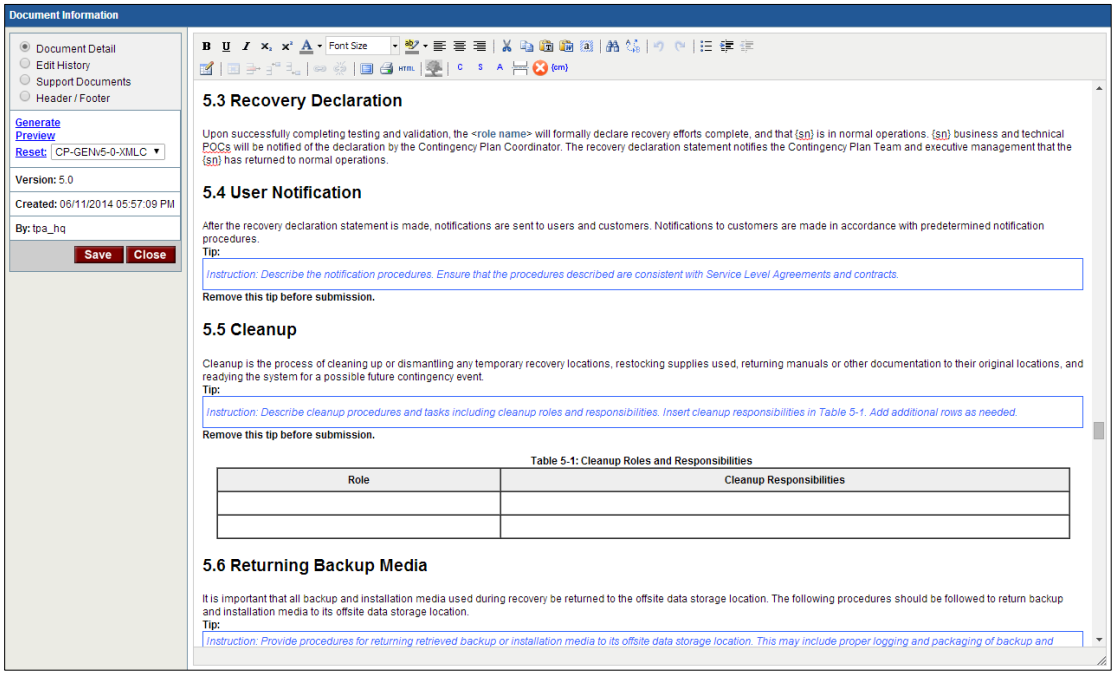


Figure 38: Built-in Content Authoring

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.

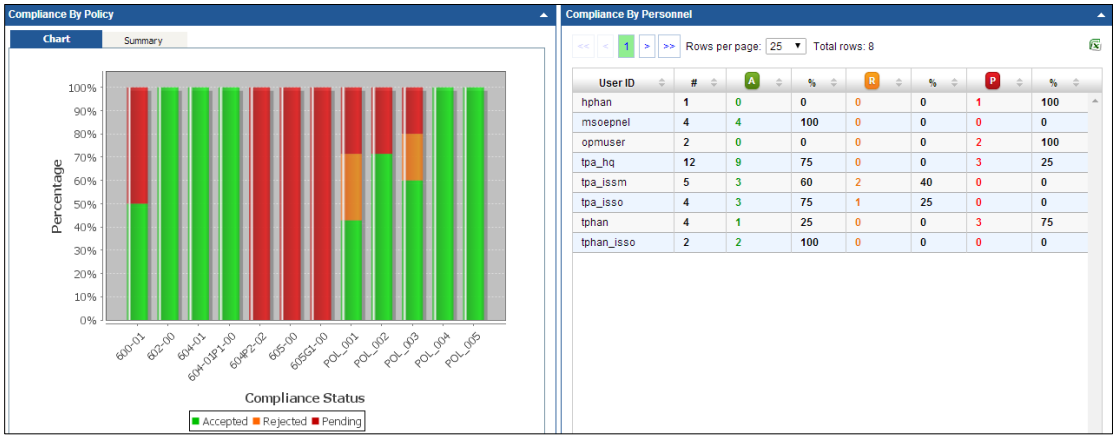


Figure 39: Policy Compliance

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. *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.* *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.*
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.

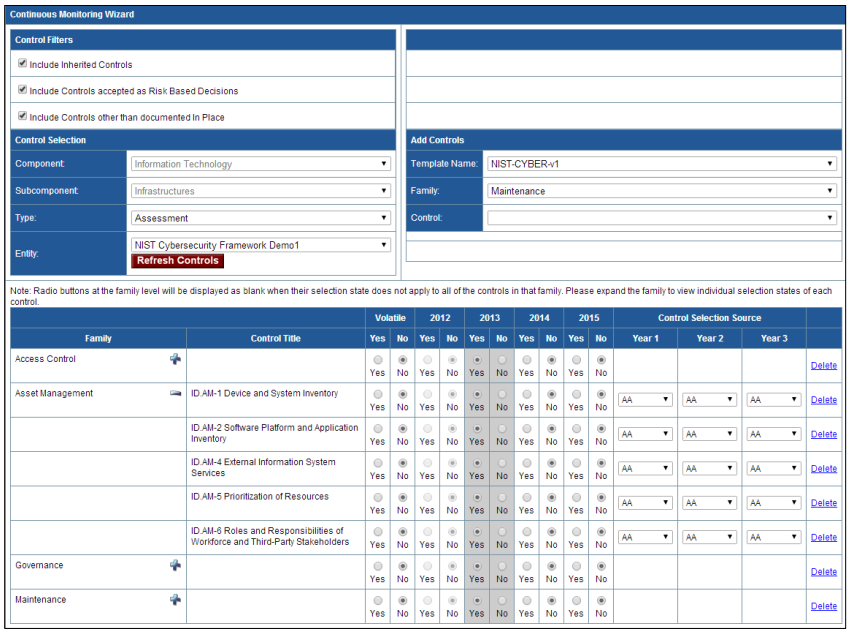


Figure 40: Continuous Monitoring Wizard

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[1] 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
Cost savings elements					
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					
Continous monitoring					
Total Values	$ -	$ 310,553	$ 116,264	$ 116,264	$ 116,264

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

[1] "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