



TrustedAgent GRC and NIST Cybersecurity Framework

NIST Cybersecurity Framework is voluntary framework to support the emerging needs for having robust and effective cyber security practices across an enterprise. This whitepaper discusses the capabilities of TrustedAgent GRC to accelerate and strengthen the implementation of an effective cybersecurity program by automating or addressing many of the practices required by the framework.



NIST cybersecurity Framework (CSF) is an outcome of government and industry collaboration to the development of a voluntary risk-based Cybersecurity Framework that describes a set of industry standards and best practices to help organizations manage cybersecurity risks. The resulting framework uses a common language to address and manage cybersecurity risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses. While the framework is intended for adoption by organizations within any of the sixteen critical infrastructure sectors, the framework can be utilized by any organization desiring to strengthen its security posture and cyber-practices.

The Framework encourages organizations to view cybersecurity impact and risk in similar consideration as:

- Financial risk
- Operational risk
- Safety risk
- Reputational risk

For organizations regulated by government agencies (FFIEC, FRB, OCC) or industry bodies (PCI) such as financial services institutions or healthcare organizations, the framework does not supersede existing regulatory requirements.

The purpose of this whitepaper is to educate the readers with the key principles of the framework, its applicability of use, and the requirements should organizations pursue adoption. The white paper also addresses the possibility of automated GRC solutions to accelerate implementation and ongoing support of cybersecurity activities for the organization.

Background

The Cybersecurity Framework is the outcome of NIST collaboration with industry contributors for almost a year. The initiative was started as the result of Executive Order (EO) 13636, and ended in February 2014 with the issuance of the framework. The final framework, v1.0, incorporated over 2,700 comments and feedbacks from road shows across five major locations throughout the US during the development period.

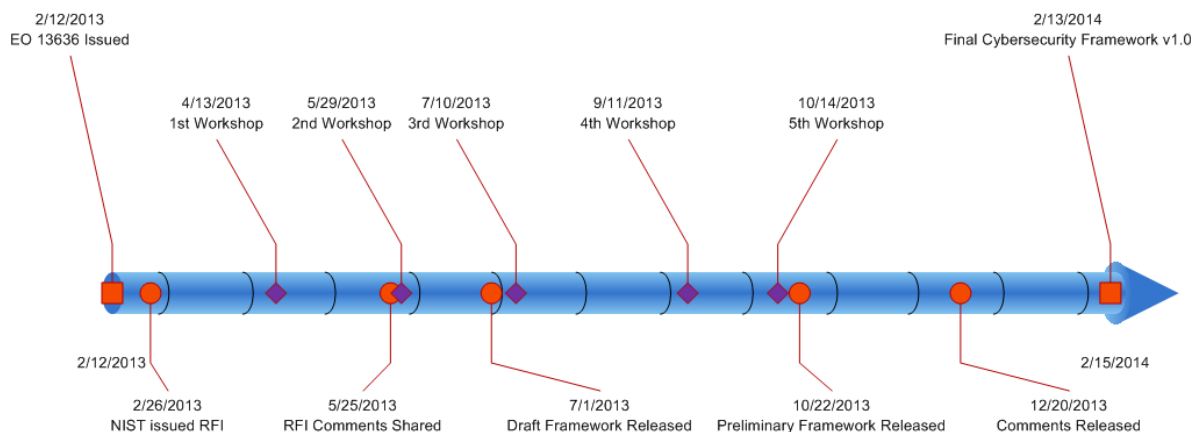


Figure 1: CSF Implementation Timeline

Per EO, the framework was delivered to be adaptable, flexible and scalable across all organizations of varying sizes, sophistication, and cybersecurity maturity while meeting the following objectives:

- Improve organization's readiness for managing cybersecurity risk
- Actionable across the enterprise
- Flexible, repeatable and performance-based
- Cost-effective
- Leverage standards, methodologies and processes
- Promote technology innovation
- Focus on outcomes

Key Components of Cybersecurity Framework

The framework consists of two major components:

- Framework Core
- Framework Implementation Tiers

The Framework Core, shown to the right, details key cybersecurity activities and key references of requirements to other industry risk management controls including NIST 800-53, COBIT, and ISA. The Core contains four elements, normalized to commonly used standards and guidelines, as follow:

- **Functions:** High-level cybersecurity activities to be developed, prioritized, and implemented.
- **Categories:** Groups of cybersecurity outcomes to be addressed.
- **Subcategories:** Specific controls or requirements to be evaluated for each of the outcomes defined in Categories.
- **Information References:** Illustrative standards, guidelines and practices from other industry frameworks or control sets.

Functions	Categories	Subcategories	Informative References
IDENTIFY	Institutional understanding to manage cybersecurity risk		
PROTECT	Safeguards to ensure delivery of CI services		
DETECT	Identify the occurrences of a cybersecurity event.		
RESPOND	Take action (address) a detected cybersecurity event		
RECOVER	Restore impaired capabilities or CI services from a cybersecurity event		

Figure 2: Framework Core

The Functions of the Core outlines the five phases of the framework where each phase carries out specific group of activities as shown above. The Functions assist the organization with defining and expressing its cybersecurity program, risk management processes, and decisions to identify, manage and remediate threats. The Functions are generalized to enable integration to internal organization cybersecurity program (if exists)

or alignment to existing methodologies for incident and risk management, and provide justifications to support investments in cybersecurity.

The Functions defined in the framework share significant similarities to other risk management approaches including NIST Risk Management Framework (RMF), COBIT and ISO 27001. The details of the overlap between frameworks may vary due to the number of elements of the phases but generally speaking as shown in the figures below, the overlaps are somewhat significant. The mappings from the framework to NIST RMF are shown below:

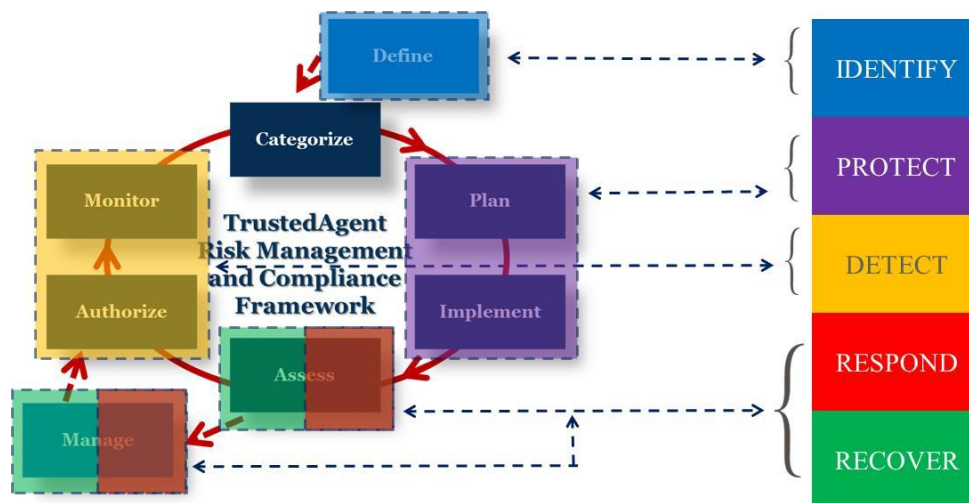


Figure 3: NIST RMF and Cybersecurity Framework

The mappings of the Cybersecurity framework to COBIT and ISO 27001 are less precise compared to RMF, due mostly in part to the differences of the domains (e.g., phases) of COBIT versus the definitions of the Functions.

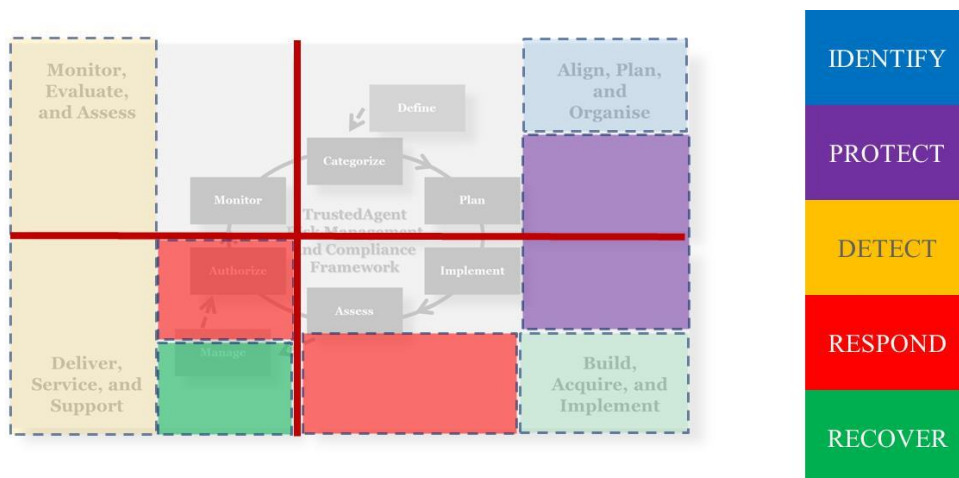


Figure 4: COBIT/ISO 27001 and Cybersecurity Framework

The second major component of the framework is the Implementation Tiers, which describes the maturity level of the organization with regard to cybersecurity practices. The Implementation Tiers drive the number

and the complexity of the requirements, and directly relate to the potential cybersecurity risk of the organization as shown below.

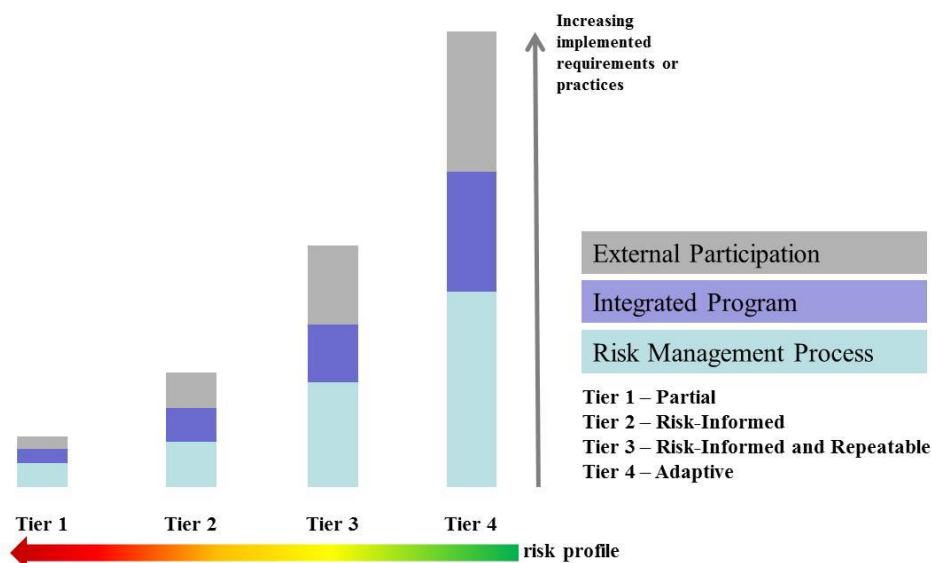


Figure 5: Implementation Tiers

A highly adaptive and mature organization at Tier 4 is expected to have effectively in place many of the required controls of the framework vs. that of a partial organization (Tier 1), where cybersecurity program is under development. The Implementation Tiers also tie to the Framework Profile which describes the progression and ongoing improvement in the organization's cybersecurity practices over time as the results of maturity of the organization, and the added-benefits to support and achieve sector goals and objectives of the organization, industry practices and other legal and regulatory requirements.



Figure 6: Framework Profile

It is noteworthy to point out that the concepts of Implementation Tiers and Organizational Profile have been adopted and implemented by several sectors. One key difference is the number of tiers defined and the number of elements from each of the tiers. The first example shown below is the Oil & Gas Sector Cybersecurity Capability Maturity Model (C2M2). This Implementation Maturity Level Model is originally derived from the Electric Sector C2M2, and therefore both models share significant similarities except for the differences in the domains. The second example highlights Institution's Maturity Profile as it applies to financial institutions under the Federal Reserve Bank's Risk-Focused Program designed for community banking institutions.

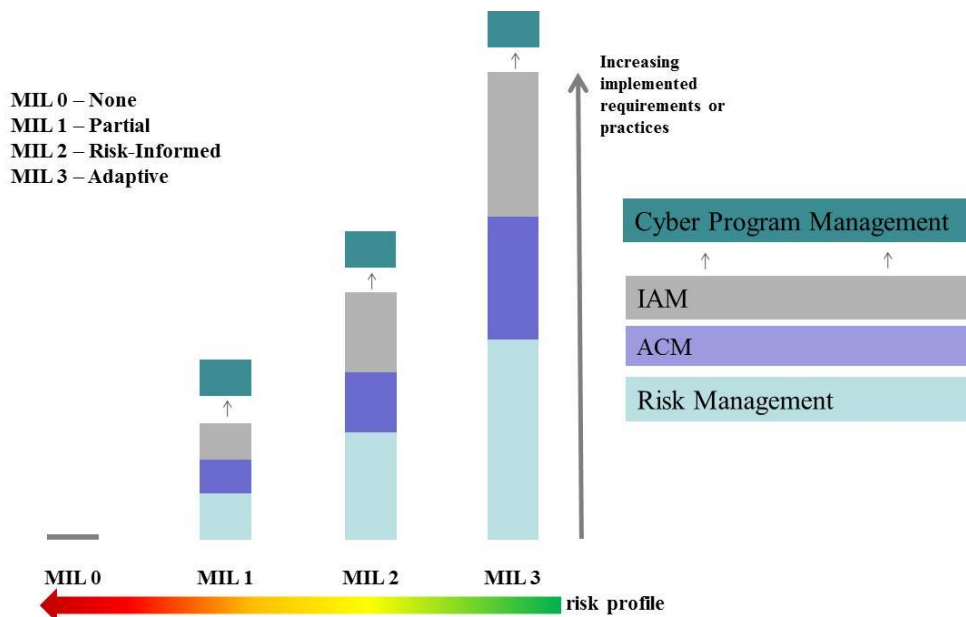


Figure 7: Oil & Gas Sector or Electric Sector C2M2

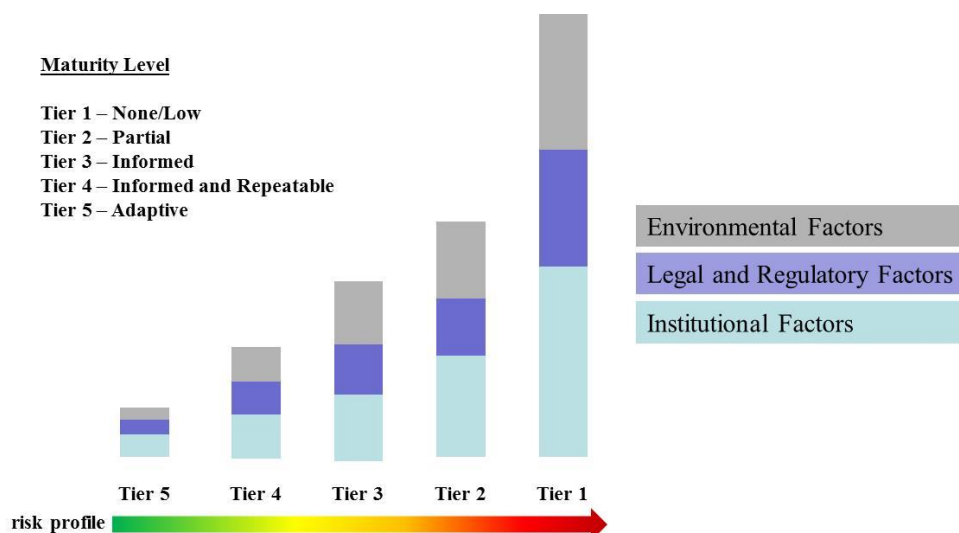


Figure 8: Institution Profile and Inherent Consumer Compliance Risk

Benefits of Framework Adoption

Enhanced cybersecurity posture as the results of improvements and consistency of practices to business processes for managing cybersecurity activities. Organizations can expect 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 cybersecurity requirements outlined in the framework can also provide or prove regulatory compliance enabling organizations to lower their regulatory and audit risk profile with regulatory bodies as well as lower cyberinsurance premiums.

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.

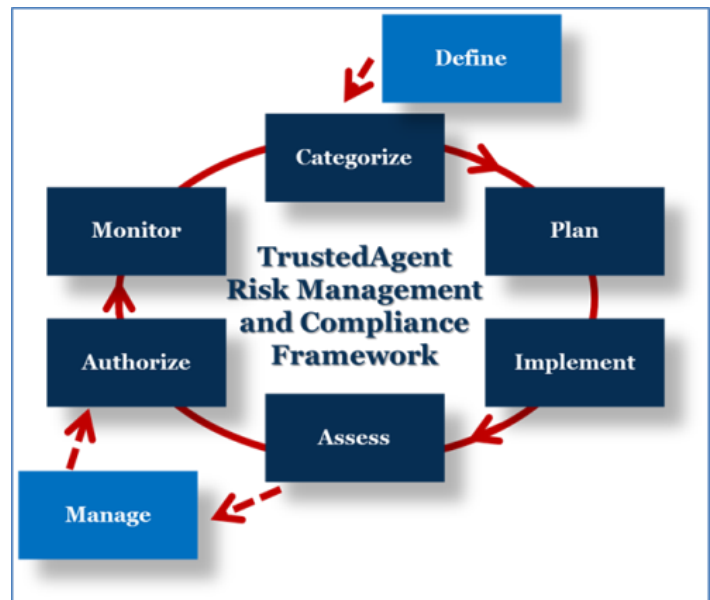
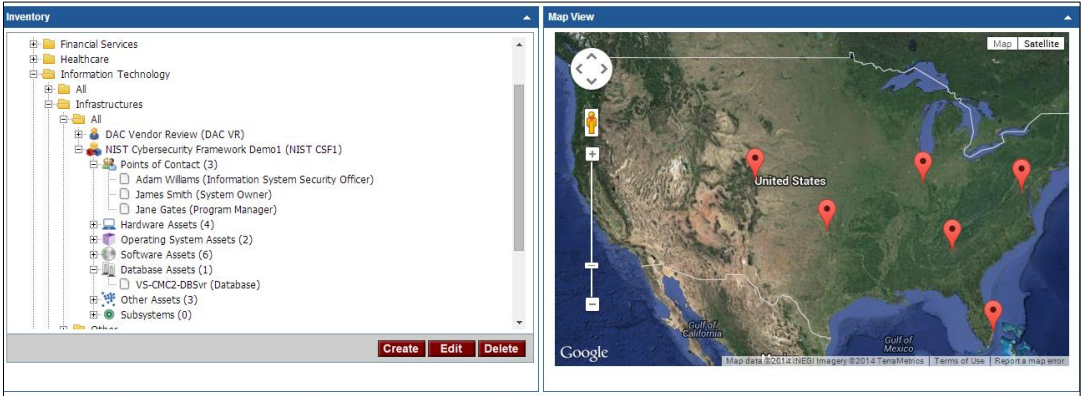
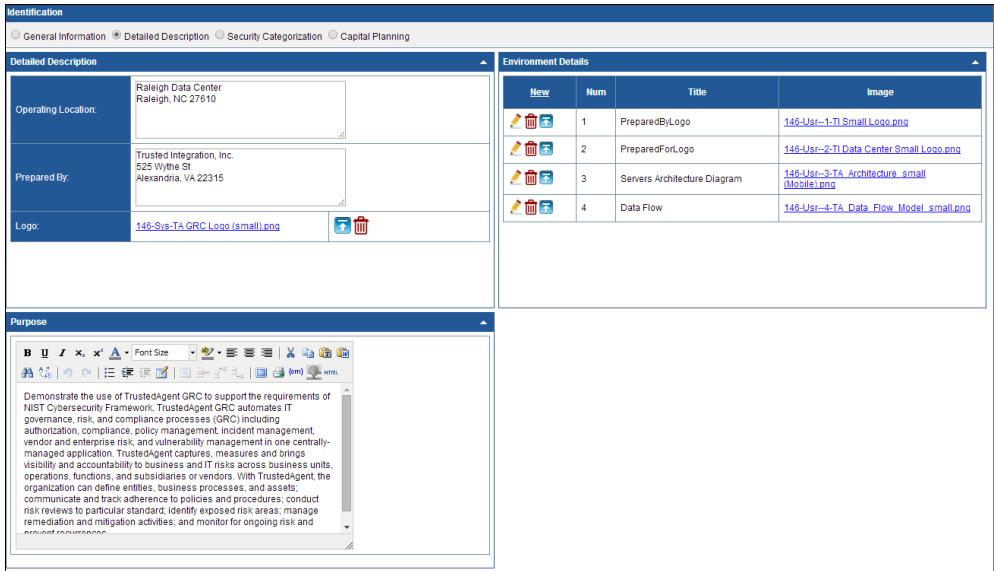
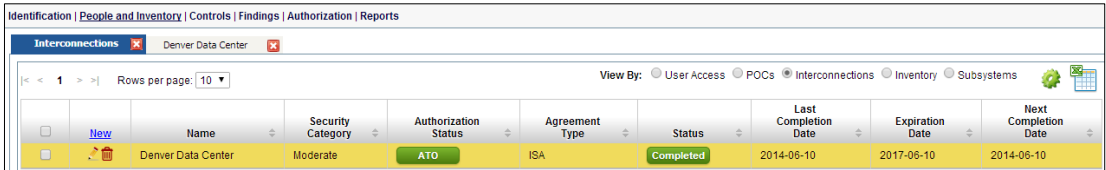


Figure 9: TrustedAgent Risk Management and Compliance Framework

TrustedAgent (TA) Risk Management and Compliance Framework is modeled after NIST Risk Management Framework (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). Each phase is further described below along with the cybersecurity requirements directly supported.

1. **Define.** Entities such as information systems, security programs, data centers or vendors are managed within TrustedAgent. Key requirements addressable by TrustedAgent to support CSF include:

Requirement	How TrustedAgent GRC Supports the Requirement
Asset Management	
ID.AM-1: Physical devices and systems within the organization are inventoried	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.

Requirement	How TrustedAgent GRC Supports the Requirement
ID.AM-2: Software platforms and applications within the organization are inventoried	 <p>Figure 10: Inventory of Entities</p>
ID.AM-3: Organizational communication and data flows are mapped	<p>TrustedAgent enables organizations to centrally manage key images and documents representing architecture and network diagrams, boundaries, workflows, interconnections, etc., and re-use across a number of key regulatory documents.</p>  <p>Figure 11: Repository of Reusable Key Diagrams</p>
ID.AM-4: External information systems are catalogued	<p>Interconnections between information systems within the organization and to external entities outside of the organization can be managed along with characteristics of the information exchange, security and service level agreements, key contacts, and the authorization of the interconnections.</p>  <p>Figure 12: Interconnections</p>

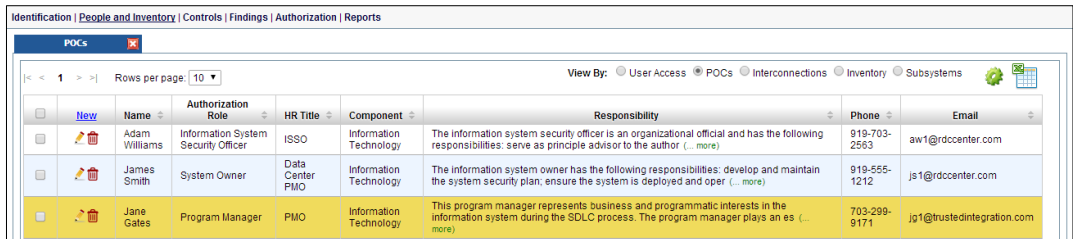
Requirement	How TrustedAgent GRC Supports the Requirement
ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on the classification, criticality, and business value	Resources (i.e., people, hardware, software, process, etc.) can be assigned to the entities that they 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 be classified as a critical asset, or financial or privacy sensitive to highlight business value to the organization. An aggregated risk score of vulnerabilities associated with an asset can be leveraged to prioritize remediation efforts.
ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	<p>TrustedAgent offers several built-in roles to support key workforce member assignment as well as custom roles defined by the organization. Standardizing roles ensure a clear assignment of roles for the workforce members in supporting authorization, maintenance, and incident response management. Suppliers, vendors, partners and customers can be tracked and managed as entities within TrustedAgent.</p> 

Figure 13: Key Contacts and Roles

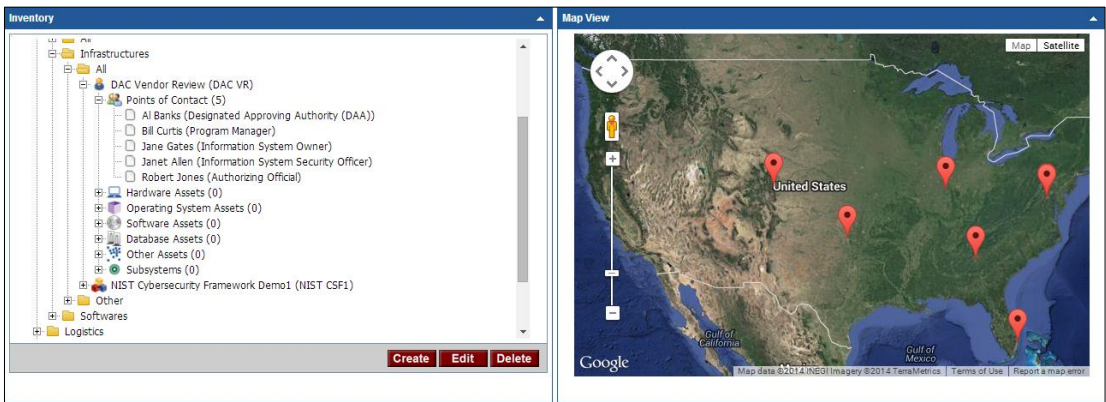
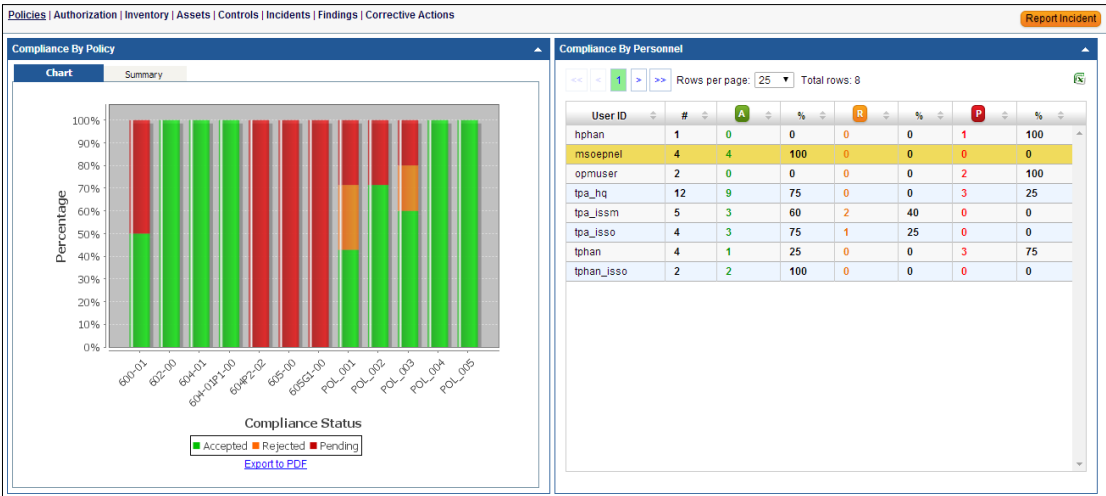
Business Environment	
ID.BE-1: The organization's role in the supply chain and is identified and communicated	<p>TrustedAgent allows organizations to manage their suppliers, vendors, and business partners/associates as vendor entities. Data centers can also be tracked as site entities. Information exchange and logistics between the organization and its suppliers can be managed through interconnections.</p> 

Figure 14: Use of Vendor Entity-Type

Requirement	How TrustedAgent GRC Supports the Requirement
ID.BE-2: The organization's place in critical infrastructure and their industry ecosystem is identified and communicated	TrustedAgent utilizes a common descriptive framework to describe cybersecurity 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.
Governance	
ID.GV-1: Organizational information security policy is established	TrustedAgent provides a repository of policies that users can leverage and customize for their organization. Additional policies can be created and published to track adherence of the policies by end-users.
ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	User roles and responsibilities can be associated with established policies in TrustedAgent which can then be published to user to track adherence of the policies by users with the assigned role and responsibilities.
 <p>Figure 15: Policy Management</p>	
Risk Management	
ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders	TrustedAgent platform serves as a technology platform to support the organization's risk management processes and related activities. Within TrustedAgent, organizations gain visibility and accountability to the risks of their entities, assets, and business processes and consistent approach to remediate and mitigate the risks.
Information Protection Processes and Procedures	
RS.IP-2: A System Development Life Cycle to manage systems is implemented	TrustedAgent supports entities through the assigned SDLC life cycle. SDLC status can be leveraged to filter reports and dashboard views.

Requirement	How TrustedAgent GRC Supports the Requirement
Anomalies and Events	
DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	TrustedAgent provides a common descriptive framework that establishes baseline configurations for information systems (ownership, characteristics, network/architecture diagrams, key contacts, risk or maturity rating, control requirements, authorization metrics, etc.) and system components (devices, applications, assets, parents) including communications (interconnections, cloud service and deployment type) and connectivity-related aspects of systems.
Detection Processes	
DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	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.
Communications	
RS.CO-2: Events are reported consistent with established criteria	TrustedAgent enables the gathering of information consistent to industry requirements from US-CERT, HHS Breach Reporting, NERC/DOE, PCI and applicable industry standards or regulations to enable the incident response team to assess and report accordingly.

2. **Categorize.** Security categorization processes are employed to determine applicable security requirements. Controls are defined based on predefined organizational templates that can be tailored across the various components and business units within the organization.

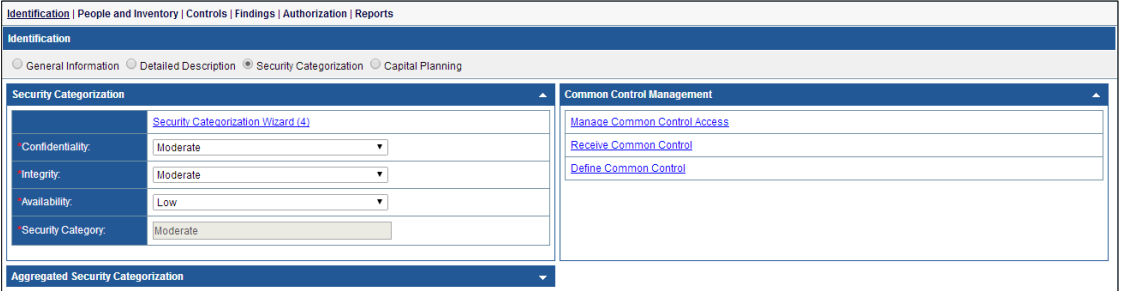
Requirement	How TrustedAgent GRC Supports the Requirement
Business Environment	
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	<p>Organizations can prioritize (or categorize) entities based the risk rating using standard methods including NIST 800-60, 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 based on NIST 800-60 thereby significantly reduces the effort to establish control baseline for control implementation and assessment.</p> 

Figure 16: Categorization

Requirement	How TrustedAgent GRC Supports the Requirement																																																							
	Business Environment																																																							
	<div>Identification People and Inventory Controls Findings Authorization Reports</div> <div>Identification</div> <div><input type="radio"/> General Information <input type="radio"/> Detailed Description <input checked="" type="radio"/> Security Categorization <input type="radio"/> Capital Planning</div> <div>Security Categorization >> Security Categorization Wizard</div> <div>List of Information Types</div> <div>The following are information types that are applicable to the application in accordance with the organization security categorization methodology.</div> <table><thead><tr><th>New</th><th>Information Category</th><th>Information Type</th><th>Name</th><th>Justification</th><th>Confidentiality</th><th>Integrity</th><th>Availability</th><th>Default Confidentiality</th><th>Default Integrity</th><th>Default Availability</th></tr></thead><tbody><tr><td></td><td>C.2.1 Controls and Oversight</td><td>C.2.1.1 Corrective Action</td><td>C.2.1.1 Controls and Oversight: Corrective Action</td><td></td><td>Low</td><td>Low</td><td>Low</td><td>Low</td><td>Low</td><td>Low</td></tr><tr><td></td><td>C.3.5 Information and Technology Management</td><td>C.3.5.3 System Maintenance</td><td>C.3.5.3 Information and Technology Management: System Maintenance</td><td></td><td>Low</td><td>Moderate</td><td>Low</td><td>Low</td><td>Moderate</td><td>Low</td></tr><tr><td></td><td>C.3.5 Information and Technology Management</td><td>C.3.5.5 Information System Security</td><td>C.3.5.5 Information and Technology Management: Information System Security</td><td></td><td>Low</td><td>Moderate</td><td>Low</td><td>Low</td><td>Moderate</td><td>Low</td></tr><tr><td></td><td>C.3.5 Information and Technology Management</td><td>C.3.5.8 System and Network Monitoring</td><td>C.3.5.8 Information and Technology Management: System and Network Monitoring</td><td></td><td>Moderate</td><td>Moderate</td><td>Low</td><td>Moderate</td><td>Moderate</td><td>Low</td></tr></tbody></table>	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
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 17: Categorization Wizard

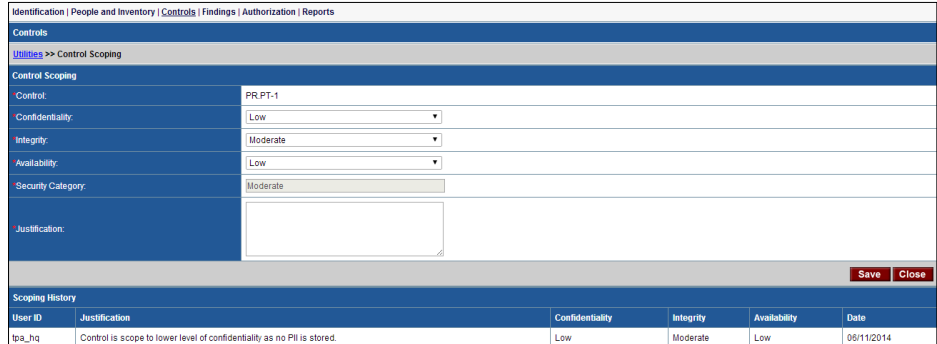
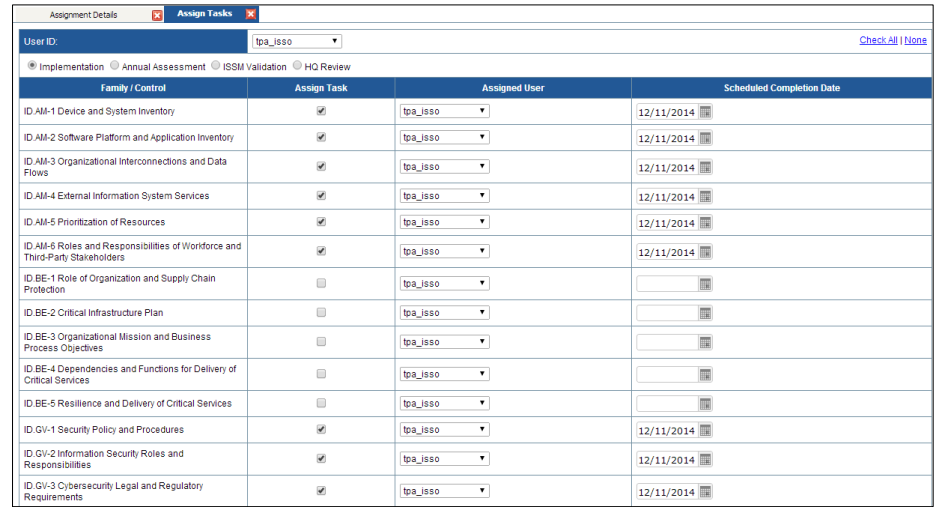
Figure 17: Categorization Wizard

3. **Plan.** Controls are assigned to support staff. Common controls are defined for the enterprise and used by various entities. Controls are tailored as needed for the entity.

Requirement	How TrustedAgent GRC Supports the Requirement																																																																																																																								
	Business Environment																																																																																																																								
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	<p>Critical entities and relationship to other entities can be defined using a parent/child or program or site relationship. Key diagrams can be incorporated in to regulatory/industry reports. Interconnections can be created to define information sharing and business relationships between entities. Common controls can be established to promote critical functions and services provided across the organization. Controls can also be scoped to the appropriate level representative of the critical services.</p>																																																																																																																								
	<table><tr><th colspan="5">Receive Common Control</th></tr><tr><th>Family</th><th>Control Title</th><th>Maps to Control</th><th colspan="2">Raleigh Data Center</th></tr><tr><td>Access Control</td><td></td><td></td><td><input checked="" type="radio"/> Inherited</td><td><input type="radio"/> None</td></tr><tr><td>Anomalies and Events</td><td></td><td></td><td><input type="radio"/> Inherited</td><td><input checked="" type="radio"/> None</td></tr><tr><td>Asset Management</td><td></td><td></td><td><input type="radio"/> Inherited</td><td><input checked="" type="radio"/> None</td></tr><tr><td>Awareness and Training</td><td></td><td></td><td><input type="radio"/> Inherited</td><td><input checked="" type="radio"/> None</td></tr><tr><td>Business Environment</td><td></td><td></td><td><input type="radio"/> Inherited</td><td><input checked="" type="radio"/> None</td></tr><tr><td>Data Security</td><td></td><td></td><td><input checked="" type="radio"/> Inherited</td><td><input type="radio"/> None</td></tr><tr><td>Detection Processes</td><td></td><td></td><td><input type="radio"/> Inherited</td><td><input checked="" type="radio"/> None</td></tr><tr><td>Governance</td><td></td><td></td><td><input type="radio"/> Inherited</td><td><input checked="" type="radio"/> None</td></tr><tr><td>Information Protection Processes and Procedures</td><td></td><td></td><td><input checked="" type="radio"/> Inherited</td><td><input type="radio"/> None</td></tr><tr><td>Maintenance</td><td></td><td></td><td><input checked="" type="radio"/> Inherited</td><td><input type="radio"/> None</td></tr><tr><td>Protective Technology</td><td></td><td></td><td><input type="radio"/> Inherited</td><td><input checked="" type="radio"/> None</td></tr><tr><td>Recovery Communications</td><td></td><td></td><td><input type="radio"/> Inherited</td><td><input checked="" type="radio"/> None</td></tr><tr><td>Recovery Improvements</td><td></td><td></td><td><input type="radio"/> Inherited</td><td><input checked="" type="radio"/> None</td></tr><tr><td>Recovery Planning</td><td></td><td></td><td><input type="radio"/> Inherited</td><td><input checked="" type="radio"/> None</td></tr><tr><td>Response Analysis</td><td></td><td></td><td><input type="radio"/> Inherited</td><td><input checked="" type="radio"/> None</td></tr><tr><td>Response Communications</td><td></td><td></td><td><input type="radio"/> Inherited</td><td><input checked="" type="radio"/> None</td></tr><tr><td>Response Improvements</td><td></td><td></td><td><input type="radio"/> Inherited</td><td><input checked="" type="radio"/> None</td></tr><tr><td>Response Mitigation</td><td></td><td></td><td><input type="radio"/> Inherited</td><td><input checked="" type="radio"/> None</td></tr><tr><td>Response Planning</td><td></td><td></td><td><input type="radio"/> Inherited</td><td><input checked="" type="radio"/> None</td></tr><tr><td>Risk Assessment</td><td></td><td></td><td><input type="radio"/> Inherited</td><td><input checked="" type="radio"/> None</td></tr><tr><td>Risk Management Strategy</td><td></td><td></td><td><input type="radio"/> Inherited</td><td><input checked="" type="radio"/> None</td></tr><tr><td>Security Continuous Monitoring</td><td></td><td></td><td><input type="radio"/> Inherited</td><td><input checked="" type="radio"/> None</td></tr></table>	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
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																																																																																																																					

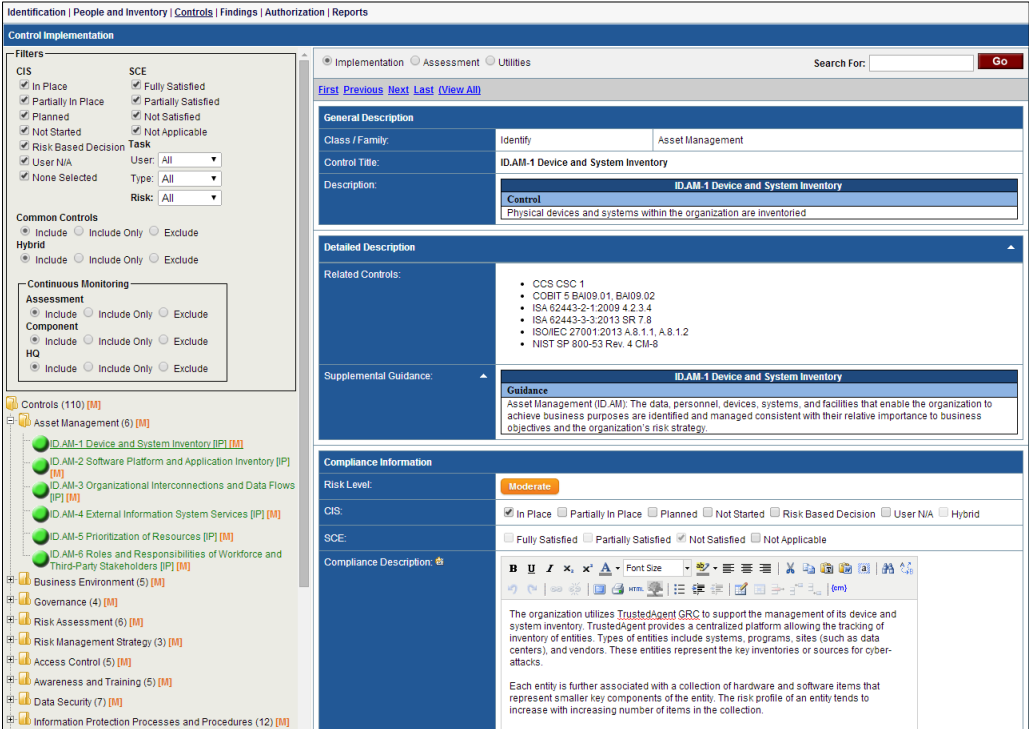
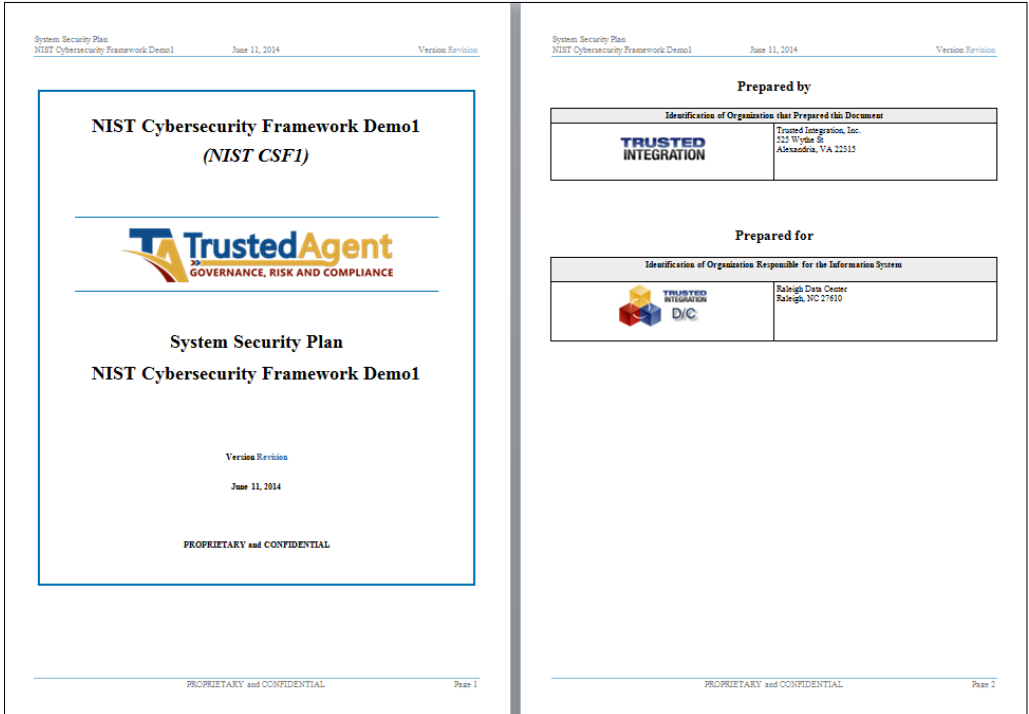
Figure 18: Receive Common Controls

Figure 18: Receive Common Controls

Requirement	How TrustedAgent GRC Supports the Requirement
	<p>Business Environment</p>  <p>Figure 19: Control Scoping</p>  <p>Figure 20: Control Assignment</p>

- Implement.** The controls are implemented and documented accordance with organizational and regulatory requirements. System security plans or other organizational documents can be generated to report on control implementation status and compliance details.

Requirement	How TrustedAgent GRC Supports the Requirement
	<p>Governance</p> <p>ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed</p> <p>TrustedAgent offers a large collection of open-source and commercial regulatory and industry standards to accelerate and maintain cybersecurity, regulatory or industry compliance program including NIST 800-53, ISO 27001, HIPAA, PCI, CIP5 and FFIEC. Adoption of TrustedAgent demonstrates the organization's commitment to address and improve cybersecurity practices. TrustedAgent supports a variety of risk management frameworks including NIST Risk Management Framework, Cybersecurity Framework, ISACA COBIT, ISO 27001, DIACAP, NERC CIP and others. The adopted frameworks can be integrated into both regulatory documentation and control content of the organization.</p> <p>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.</p>

Requirement	How TrustedAgent GRC Supports the Requirement
ID.GV-4: Governance and risk management processes address cybersecurity risks	
	

5. **Assess.** Controls are assessed by independent assessors. Control Assessment Plan, 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 that are accepted and converted to corrective actions where they are tracked for remediation purposes.

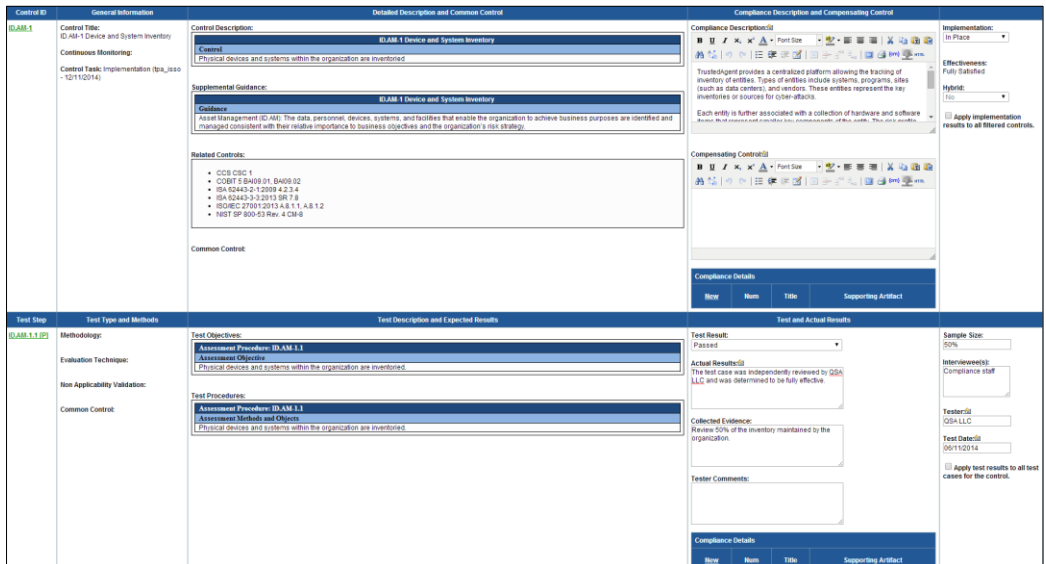
Requirement		How TrustedAgent GRC Supports the Requirement	
Business Environment			
ID.BE-1: The organization's role in the supply chain and is identified and communicated	Audits and vendor risk assessments to identify and understand the risk and ongoing remediation can be performed to monitor supplier compliance and performance to safeguard the supply chain. Resiliency requirements can be added to compliance requirements of critical services providers and assessed periodically for effectiveness.		
ID.BE-5: Resilience requirements to support delivery of critical services are established	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 is fully supported to ensure independent review of the assessment process.		
			
Risk Assessment			
ID.RA-1: Asset vulnerabilities are identified and documented	TrustedAgent offers integrated vulnerability assessment (VA) tools to scheduling and conduct scans on demand or as scheduled 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 (configuration mapping file).		

Figure 24: Asset Inventory

Figure 25: Vulnerabilities by Risk Level and Asset Group

DE.AE-2: Detected events are analyzed to understand attack targets and methods

When integrated or combined with supported vulnerability assessment (VA) scanning applications, TrustedAgent provides end-to-end management of entities and their assets of threat events and vulnerabilities ensuring ongoing remediation of vulnerable assets and reported incidents. TrustedAgent also supports continuous monitoring of key controls and scheduled/on-demand scanning of assets using supported VA tools.

Figure 26: Integrated Vulnerability Management

Requirement	How TrustedAgent GRC Supports the Requirement
Detection Processes	
DE.DP-2: Detection activities comply with all applicable requirements	TrustedAgent supports VA scanning tools and non-technical assessments under a risk management framework, including NIST RMF, COBIT, or ISO. Risk and security rating can be performed using NIST 800-60, or PII. Privacy assessments can also be supported using NIST privacy or HIPAA controls using a privacy risk management framework consisting of privacy threshold analysis (PTA) and privacy impact assessment (PIA).
DE.DP-3: Detection processes are tested	TrustedAgent provides a separate assessment view and user role enabling an assessor independent from the business owner to conduct verification of control implementation to determine control effectiveness. This process addresses conformity assessment approach recommended by NIST Cybersecurity framework and other risk management frameworks such as FFIEC (applicable to financial institutions), PCI, FedRAMP and ISO.

6. **Manage.** 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. Corrective actions are generated for accepted findings. Corrective actions and milestones are created for controls that are not Fully Satisfied and where risks have not been accepted by the authorizing official.

Executive Summary or other organizational documents including privacy documents can be created from predefined templates to document the recommendation for the authorization of the entity.

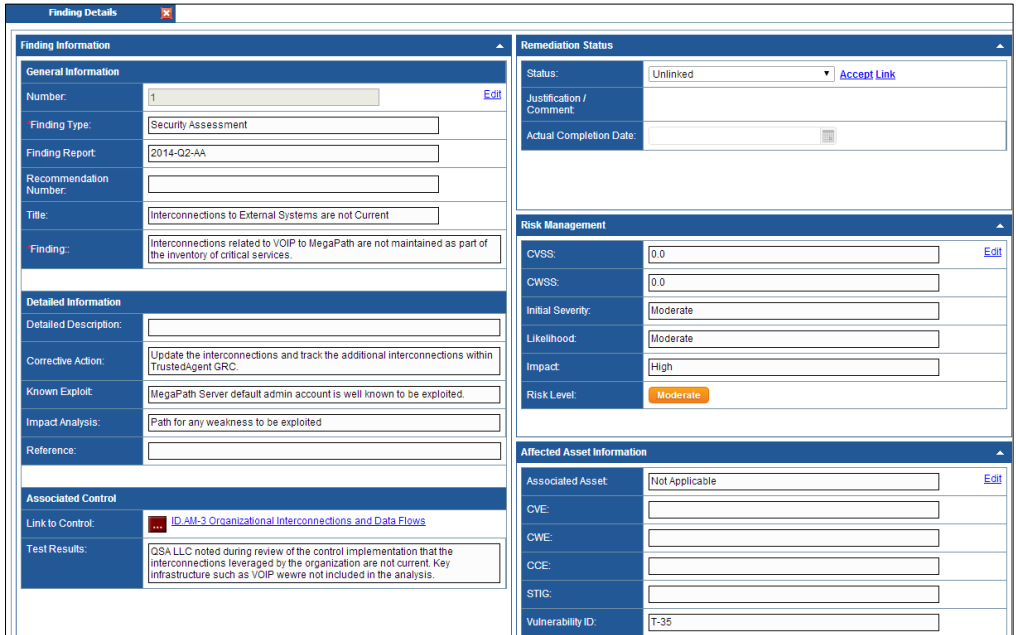
Requirement	How TrustedAgent GRC Supports the Requirement
Risk Assessment	
ID.RA-3: Threats, both internal and external, are identified and documented	<p>TrustedAgent supports threat assessment of assets through integrated and supported VA tools. Self-assessments and audits can also be conducted qualitatively using provided regulatory requirements or content provided with the selected risk management framework of the organization.</p> 

Figure 27: Finding Identification and Analysis

Requirement

ID.RA-4: Potential business impacts and likelihoods are identified

How TrustedAgent GRC Supports the Requirement

Identified findings are comprehensively supported with business impact analysis and recommended remediation action along with the assigned risk exposure level based on likelihood and impact levels.

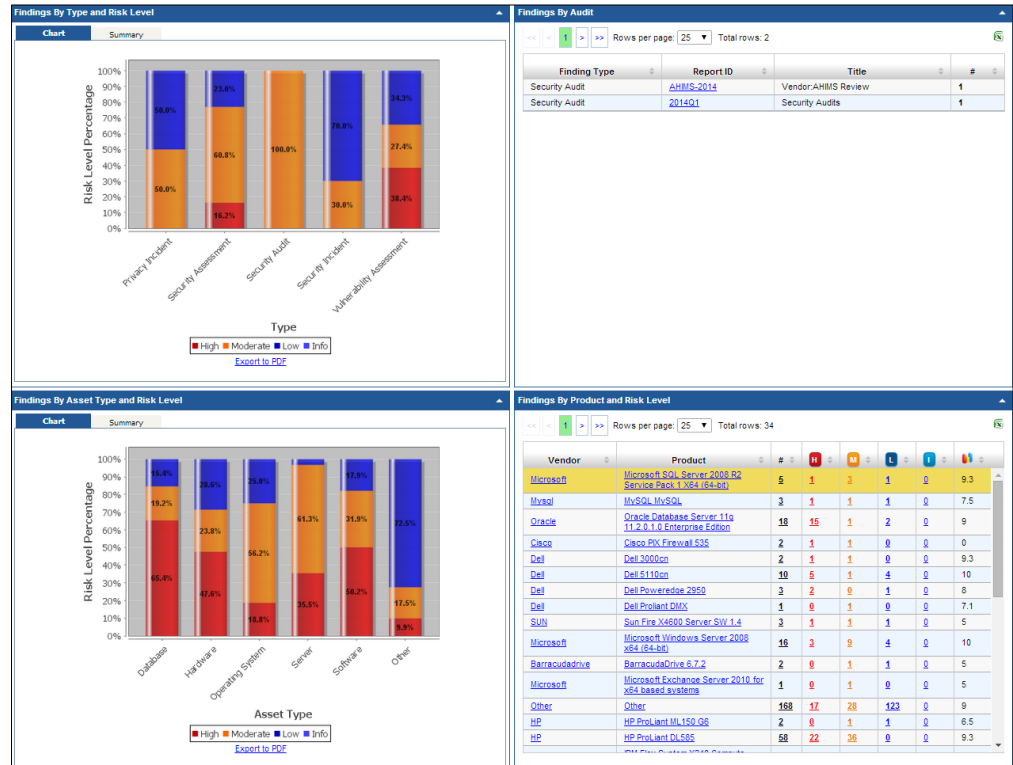


Figure 28: Findings by Type, Risk Level, and Product Group

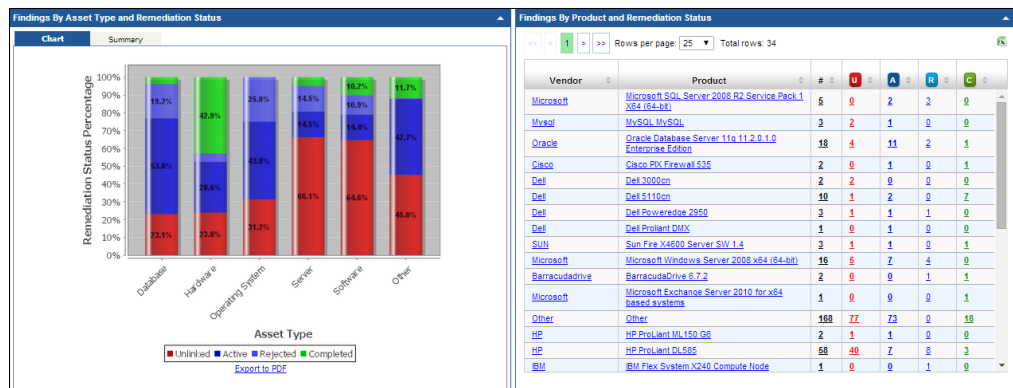
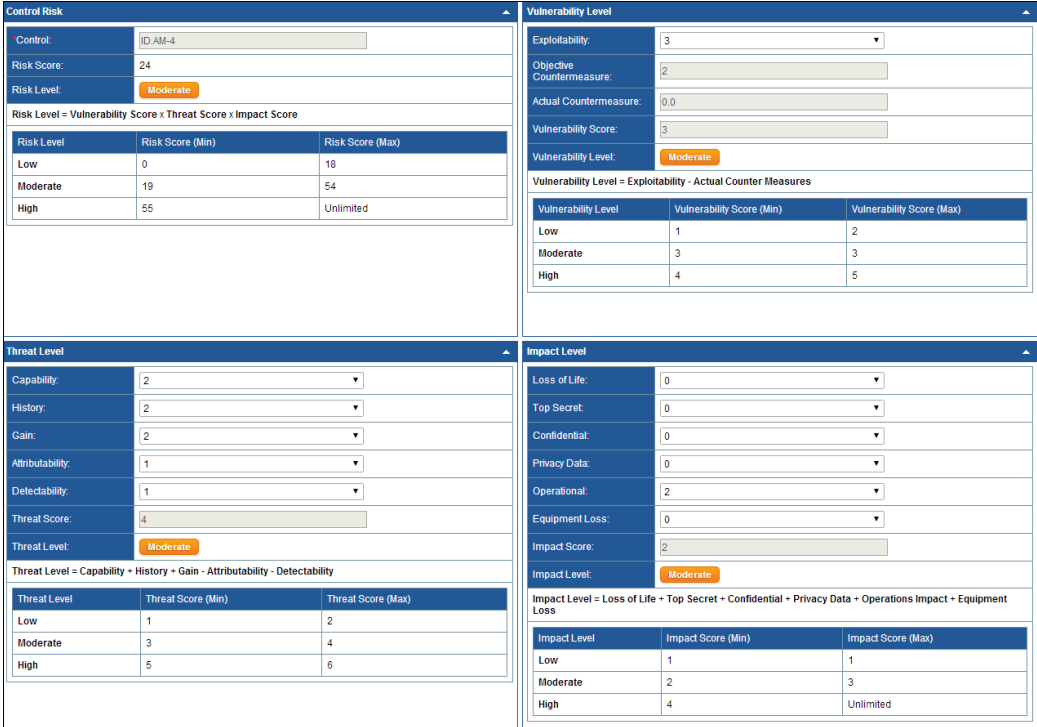


Figure 29: Findings by Remediation Status and Product Group

Requirement	How TrustedAgent GRC Supports the Requirement										
ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	TrustedAgent supports complete life cycle management of findings and corrective actions (i.e., unlinked, active, in-progress, delayed, completed, etc.). Once identified risk can be categorized by likelihood, impact, and risk level. Corrective actions with appropriate risk level can be created to manage the remediation of risks.										
ID.RA-6: Risk responses are identified and prioritized	TrustedAgent’s dashboard also provides real-time updates to findings and corrective actions as status of the risks and their remediation progress change. The dashboard is filterable and drillable to smaller organizational units and entity.										
	<div><div><div><div><div>General Information</div><div><div>Number:1</div><div>Class:Identify</div><div>Family:Asset Management</div><div>Corrective Action ID:NIST CSF1_Q3_2014_1</div><div>Finding(s):1 - Interconnections to External Systems are not Current</div><div><div>Finding (Details):<div>Finding 1 - Interconnections to External Systems are not Current Interconnections related to VOIP to MegaPath are not maintained as part of the inventory of critical services.</div><div>Inventory of interconnections supporting critical services needs to be updated and maintained so that complete assessment can be performed to evaluate organization-wide risk profile.</div></div></div><div>Description:</div></div></div><div><div>Milestones</div><table><thead><tr><th>New</th><th>No.</th><th>Milestone</th><th>Scheduled Completion Date</th><th>Status</th></tr></thead><tbody><tr><td></td><td>1</td><td>Interconnection and Vendor Service Agreement to be updated.</td><td>06/30/2014</td><td>In Progress</td></tr></tbody></table></div><div><div>Project Management</div><div><div>Status:</div><div>In Progress</div></div><div><div>Creation Date:</div><div>06/11/2014</div></div><div><div>Identified Date:</div><div>06/11/2014</div></div><div><div>Planned Start Date:</div><div></div></div><div><div>Actual Start Date:</div><div></div></div><div><div>Scheduled Completion Date:</div><div>07/31/2014</div></div><div><div>Estimated Completion Date:</div><div>07/31/2014</div></div><div><div>Actual Completion Date:</div><div>07/31/2014</div></div></div></div></div></div>	New	No.	Milestone	Scheduled Completion Date	Status		1	Interconnection and Vendor Service Agreement to be updated.	06/30/2014	In Progress
New	No.	Milestone	Scheduled Completion Date	Status							
	1	Interconnection and Vendor Service Agreement to be updated.	06/30/2014	In Progress							
	<div><div><div><div><div>Corrective Actions Opened</div><div><div>Chart</div><div>Summary</div></div><div></div></div></div><div><div><div>Corrective Actions Closed</div><div><div>Chart</div><div>Summary</div></div><div></div></div></div><div><div><div>Corrective Actions Timeliness</div><div><div>Chart</div><div>Summary</div></div><div></div></div></div><div><div><div>Corrective Actions Aging</div><div><div>Chart</div><div>Summary</div></div><div></div></div></div></div></div>										
	Figure 30: Corrective Action and Remediation										
	<div><div><div><div><div>Corrective Actions Opened</div><div><div>Chart</div><div>Summary</div></div><div></div></div></div><div><div><div>Corrective Actions Closed</div><div><div>Chart</div><div>Summary</div></div><div></div></div></div><div><div><div>Corrective Actions Timeliness</div><div><div>Chart</div><div>Summary</div></div><div></div></div></div><div><div><div>Corrective Actions Aging</div><div><div>Chart</div><div>Summary</div></div><div></div></div></div></div></div>										
	Figure 31: Corrective Action Dashboard										

Requirement	How TrustedAgent GRC Supports the Requirement
<div data-bbox="732 231 935 258">Risk Management</div>	
<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>	<p>TrustedAgent's template authoring allows the organization to define or revise controls associated with the selected framework with organization-specific requirements, response/implementation standards, and best practices. TrustedAgent enables risk tolerance to be defined at control level and be based on specific control templates defined to the CI sector. Risk tolerance may also be impacted based by the cybersecurity maturity of the organization. By default the control templates deployed are preset with risk levels commensurate to the CI sector. The control's risk level, if required, can be updated to match other values for other CI sectors.</p> <p>Organization may also adjust the actual risk level of the implemented control to commensurate to applicable risks, the extent of impact, and control implementation.</p> <div data-bbox="459 619 1490 1341">  </div>
<div data-bbox="711 1415 956 1442">Anomalies and Events</div>	
<p>DE.AE-4: Impact of events is determined</p> <p>DE.AE-5: Incident alert thresholds are established</p>	<p>TrustedAgent's incident and finding management modules allow 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.</p> <p>Incident investigation details and business impact analysis, including threat types, likelihood, impact level, and resulting risk exposure level can be documented. One or more findings can be associated to finding reports as part of a continuous monitoring program, a specific security or privacy incident, or due to a specific external audit.</p> <p>Through risk mitigation discussion with entity's business owner and oversight staff, findings exceeding risk tolerance defined for the organization 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.</p>

Requirement

How TrustedAgent GRC Supports the Requirement

Contact Information	Incident Details	Data Breach Details	Remediation Taken	Breach Notification						
Step 3. Incident Details Please provide as much detail about the incident as possible. These details are critical to helping us understand the nature of the incident and impact it may have. This information also helps us provide an appropriate response to the incident.										
Description of the incident: Patient Complaint Management system (web facing) is experiencing a DoS attack, intermittently impact performance of the server, and also prevents legitimate patient inquiries to be submitted.										
How was the incident identified: Administrator										
Type of incident: IT Incident										
Location of incident: <input type="checkbox"/> Laptop <input type="checkbox"/> Desktop <input checked="" type="checkbox"/> Server <input type="checkbox"/> Email <input type="checkbox"/> Portable Electronic Device <input type="checkbox"/> Paper <input type="checkbox"/> Electronic Medical Record <input type="checkbox"/> Other, please describe:										
Impacted by the incident: <table border="1"> <tr> <th>Number of Computers</th> <th>Number of Sites</th> <th>Number of Users</th> </tr> <tr> <td>0</td> <td>1</td> <td>0</td> </tr> </table>					Number of Computers	Number of Sites	Number of Users	0	1	0
Number of Computers	Number of Sites	Number of Users								
0	1	0								
Component impacted by the incident: Information Technology										
Subcomponent impacted by the incident: All										
Entity impacted by the incident: All										
Support Documents:										
Step 4. Affected Asset Details Please provide information about the affected asset.										
Hostname or IP Address of the affected asset: pcms.myhospitals.com										
Port(s) impacted on the affected asset: 80										
Description of the affected asset:										
Step 5. Attacker Details Please provide information about the attacker.										
Description of the attack method and protocol used: Denial of Service attack										
Hostname or IP Address used by the attacker:										
Port(s) used by the attacker:										

Figure 33: 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 attack, 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 34: List of Incidents



Figure 35: Incident Metrics

Analysis

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

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.

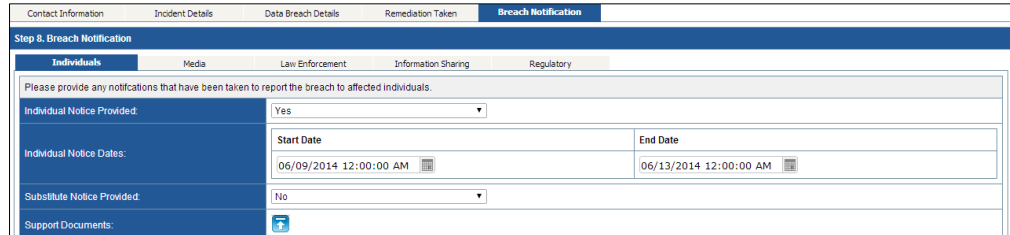


Figure 36: Incident Notifications

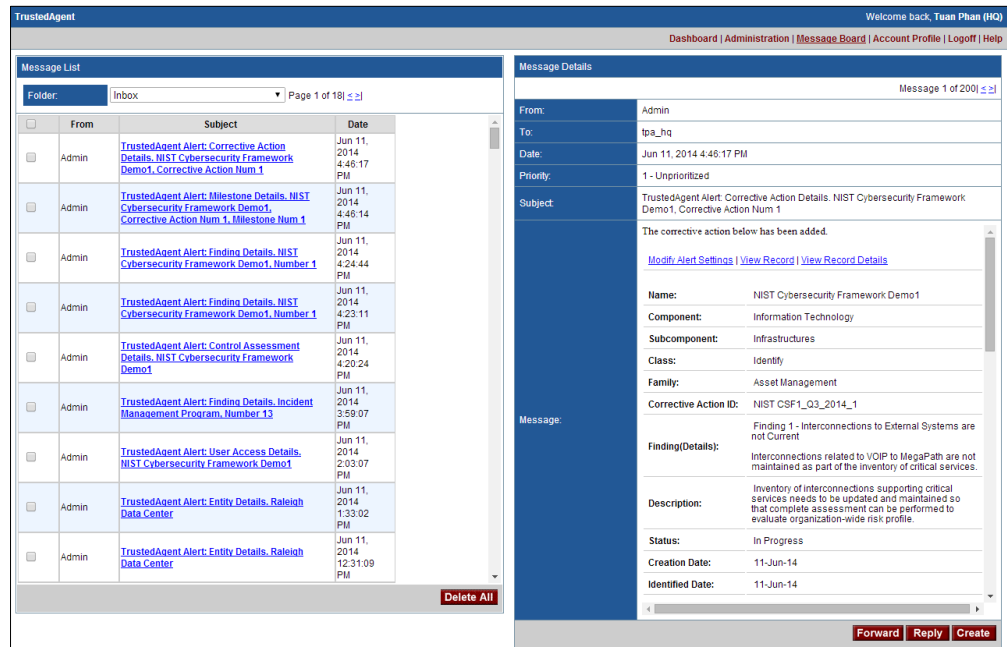
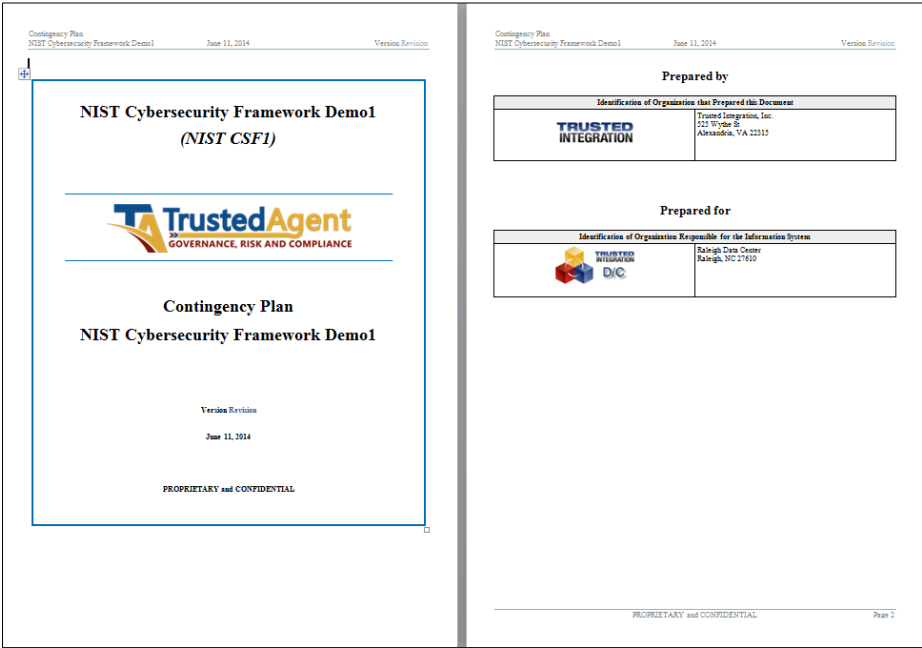
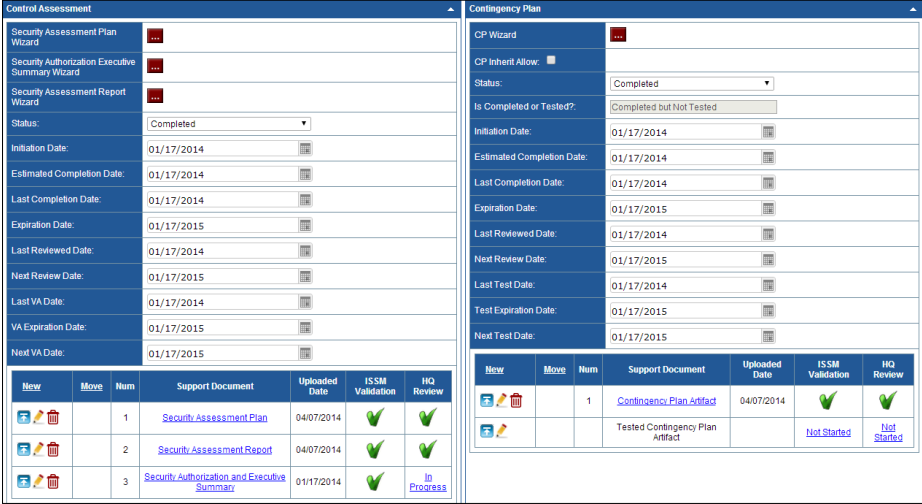


Figure 37: Message Board Notifications

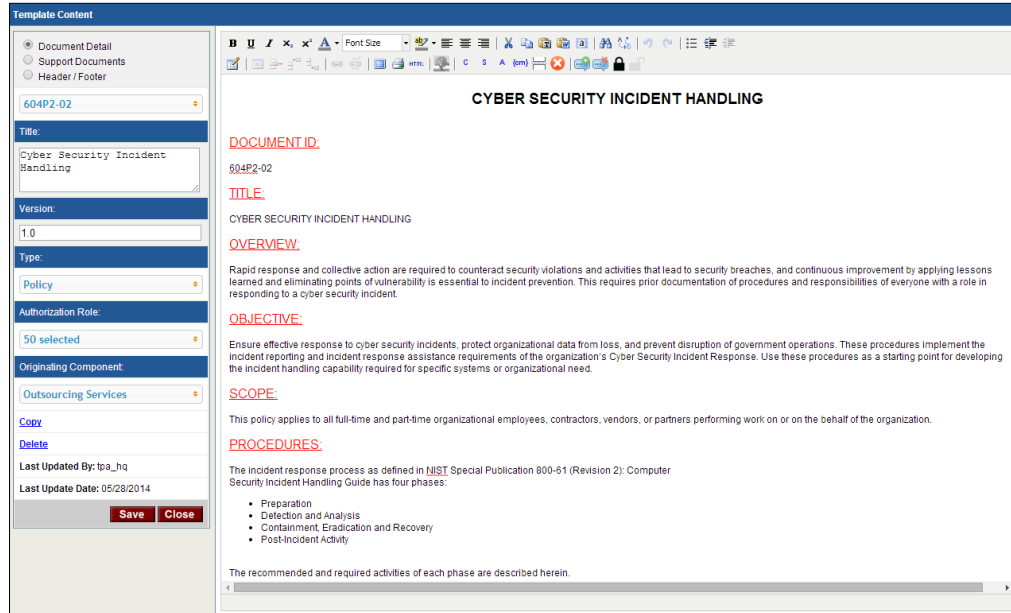
7. **Authorize.** The authorization package is presented to the authorizing official for review and approval. Approval letters and waivers are created from predefined templates that document the accreditation decision for the entity along with residual risks that was accepted and granted. Assessment 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.

Requirement	How TrustedAgent GRC Supports the Requirement
	Business Environment
ID.BE-5: Resilience requirements to support delivery of critical services are established	<p>For each of the organization's entities, contingency plan can be implemented and refined to meet specific resiliency requirements for the entity. The contingency plan may be maintained with relevant performance metrics (expiration and test dates, status, supporting artifacts).</p> <div>  </div> <p>Figure 38: Automate Contingency Plan</p> <div>  </div> <p>Figure 39: Maintain Performance Metrics</p>

Information Protection Processes and Procedures

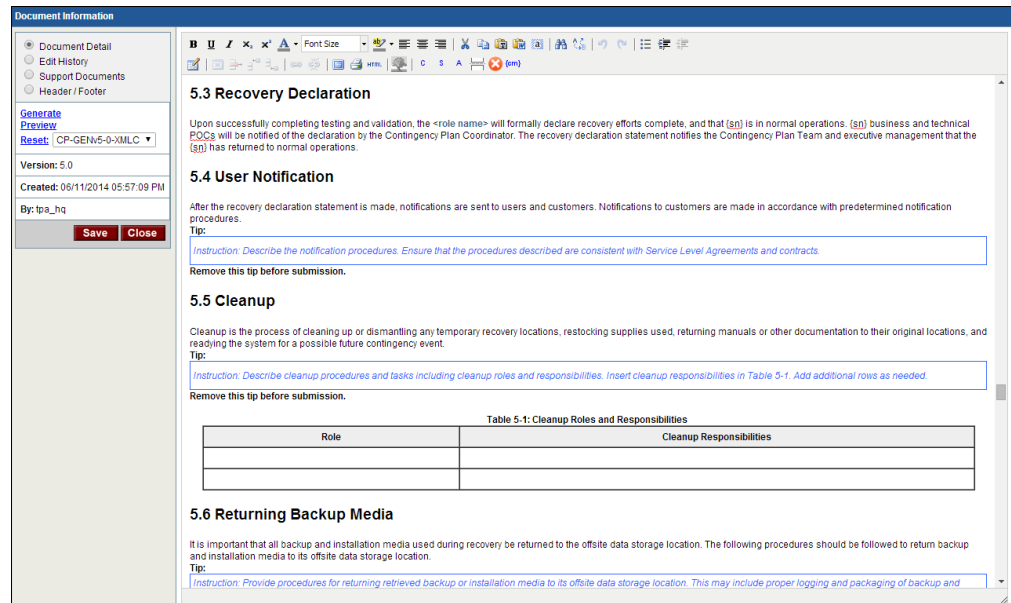
PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed

TrustedAgent provides generic incident response and business continuity policies, procedures, and plans for organizations to leverage to ensure rapid implementation. TrustedAgent also supports customization of the documents for changes based on organization's requirements. The documents can be generated in real-time with key information maintained by the organization for the entities.



The screenshot shows a web-based editor for a document titled "CYBER SECURITY INCIDENT HANDLING". On the left is a sidebar with fields for Document Detail, Support Documents, Header/Footer, Title (Cyber Security Incident Handling), Version (1.0), Type (Policy), Authorization Role (50 selected), Originating Component (Outsourcing Services), and buttons for Copy, Delete, Last Updated By, and Last Update Date. The main content area has a rich text editor with sections: DOCUMENT ID (604P2-02), TITLE (CYBER SECURITY INCIDENT HANDLING), OVERVIEW (Rapid response and collective action are required to counteract security violations...), OBJECTIVE (Ensure effective response to cyber security incidents...), SCOPE (This policy applies to all full-time and part-time organizational employees...), and PROCEDURES (The incident response process as defined in NIST Special Publication 800-61...).

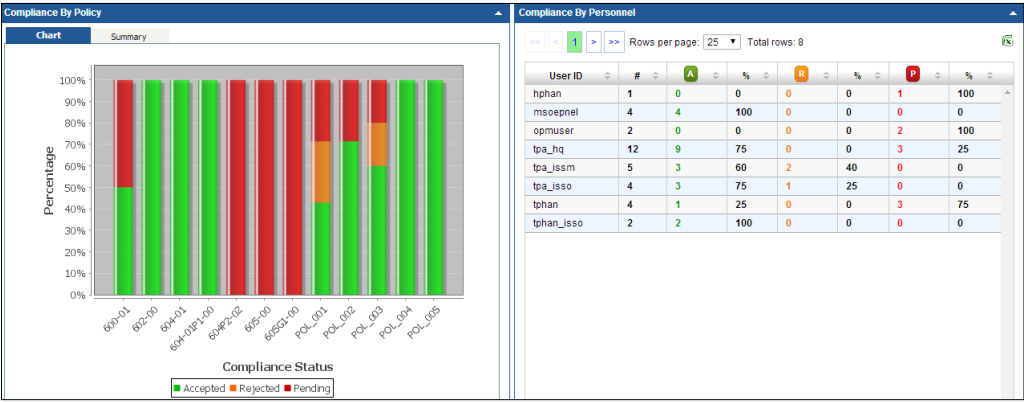
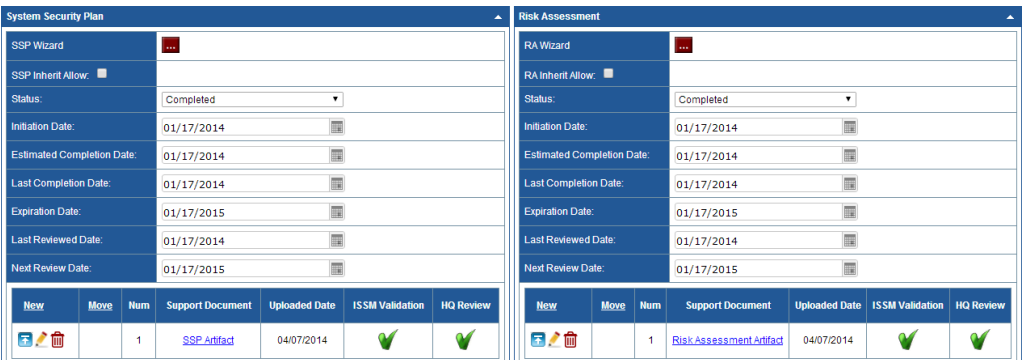
Figure 40: Centrally-Managed Policies and Procedures



The screenshot shows a web-based editor for a document titled "5.3 Recovery Declaration". The left sidebar includes Document Detail, Edit History, Support Documents, Header/Footer, Generate Preview, Reset (CP-GENV5-0-XMLC), Version (5.0), Created (05/11/2014 05:57:09 PM), and By (tpa_hq). The main content area contains sections: 5.3 Recovery Declaration (Upon successfully completing testing and validation...), 5.4 User Notification (After the recovery declaration statement is made, notifications are sent to users and customers...), 5.5 Cleanup (Cleanup is the process of cleaning up or dismantling any temporary recovery locations...), and 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...). A table titled "Table 5.1: Cleanup Roles and Responsibilities" is included with columns for Role and Cleanup Responsibilities.

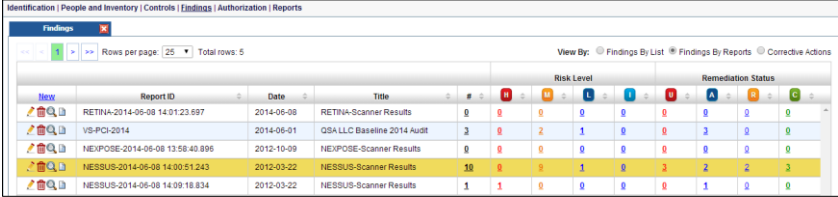
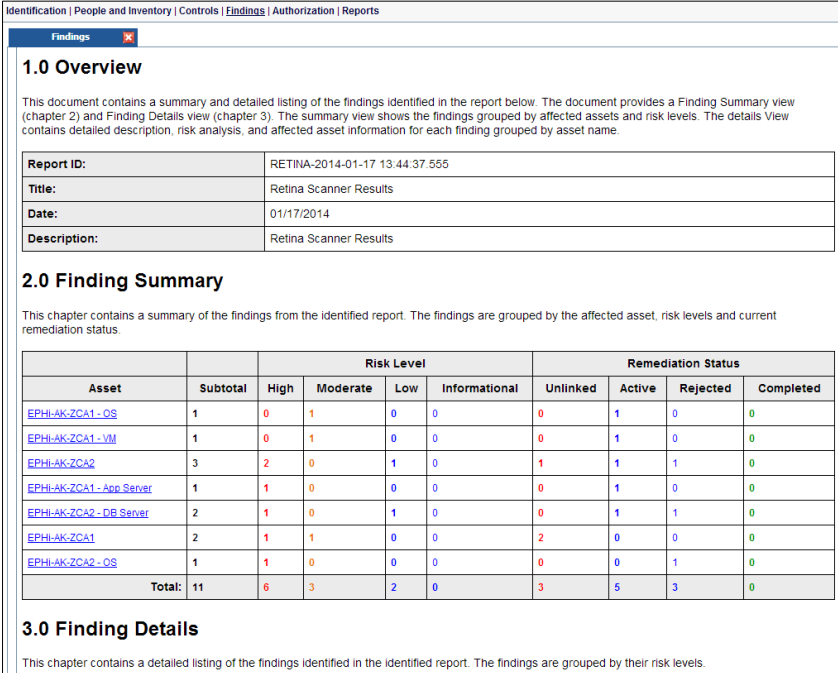
Figure 41: Built-in Content Authoring

Key performance metrics including adherence, status, scheduled completion date, and test date can also be tracked with the entity and the applicable document along with any supporting artifacts.

Requirement	How TrustedAgent GRC Supports the Requirement
	<p align="center">Business Environment</p>  <p align="center">Figure 42: Policy Compliance</p> 
PR.IP-12: A vulnerability management plan is developed and implemented	<p>TrustedAgent's out-of-the-box deployment of CSF also contains a vulnerability management plan. Organizations can leverage TrustedAgent to further customize the plan based on organization's requirements. TrustedAgent also provides technical capabilities to further manage vulnerabilities in supporting the vulnerability management plan through integrated vulnerability assessment (VA) tools or through import XML results from VA tools.</p>

8. **Monitor.** 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.

Requirement	How TrustedAgent GRC Supports the Requirement
	<p align="center">Risk Management</p>
ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders	<p>TrustedAgent platform serves as a technology platform to support the organization's risk management processes and related activities. Within TrustedAgent, organizations gain visibility and accountability to the risks of their entities, assets, and business processes and consistent approach to remediate and mitigate the risks.</p>

Requirement	How TrustedAgent GRC Supports the Requirement
Data Security	
PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	Assets associated with an entity can be updated or removed directly using TrustedAgent's asset management module, or be modified using Excel data template import, or be updated through supported vulnerability assessment tools. Findings or vulnerabilities associated with any removed asset may either require justification to close, or be transferred (assigned) to the replacement asset to provide the regulatory evidence to demonstrate ongoing compliance.
PR.DS-7: Unnecessary assets are eliminated	SDLC status can be assigned to entities allowing the entities to be managed accordingly to their lifecycle. For entities that are no longer in use (e.g., with SDLC of disposal), they can be filtered from the dashboard views allowing the key metrics to be updated to exclude these entities and the related assets.
Security Continuous Monitoring	
DE.CM-1: The network is monitored to detect potential cybersecurity events	TrustedAgent integrates with OpenVAS and SAINT vulnerability assessment scanners allowing scheduled scanning of assets for vulnerabilities, associated identified vulnerabilities to impacted assets, and creation of findings to ongoing remediation. XML results from other VA scanning tools can be filtered based on severity and imported into TrustedAgent for ongoing remediation.
DE.CM-8: Vulnerability assessments are performed	 <p>Figure 43: Finding Reports</p> 

Requirement	How TrustedAgent GRC Supports the Requirement
	<p>3.1 Asset Name: EPHI-AK-ZCA1</p> <p>3.1.1 Seagate Embedded Driver Multiple Vulnerabilities (2681578) - .NET - 2656411</p> <p>Risk Level: High CVSS: 9.3</p> <p>Remediation Status</p> <p>Status: Unlinked</p> <p>General Information</p> <p>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.</p> <p>Detailed Information</p> <p>Back to Summary Back to Top</p> <p>3.1.2 GPU-Accelerated CHIP supporting Adobe Products Multiple Vulnerabilities (20120328) - Adobe AIR x64</p> <p>Risk Level: Moderate CVSS: 6.2</p> <p>Remediation Status</p> <p>Status: Unlinked</p> <p>General Information</p> <p>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.</p> <p>Detailed Information</p> <p>Corrective Control</p> <p>Ensure that Adobe products are patched as required.</p> <p>Impact Analysis</p> <p>Category II</p> <p>Risk Management</p> <p>Likelihood: Moderate</p>

Figure 44: Online View of Finding Report

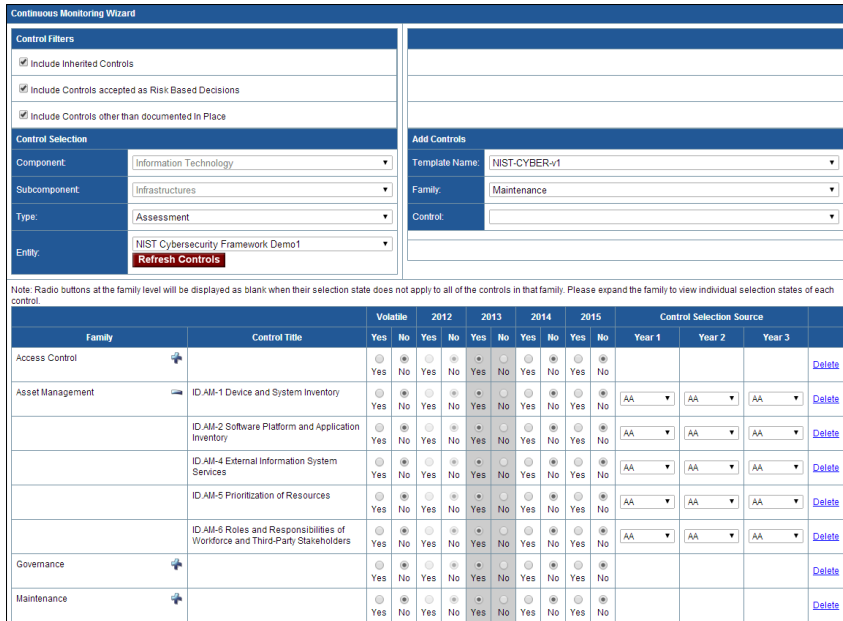
Detection Processes	
DE.DP-5: Detection processes are continuously improved	<p>Integrated vulnerability assessment tools including OpenVAS and SAINT Scanner are periodically updated according to the vendor's specification from industry vulnerability feeds. TrustedAgent also integrates it CPE to NIST NVD and CPE. Additionally, continuous monitoring wizard enables organizations to retest key controls to support ongoing compliance or organization's continuous improvement to another maturity level (i.e., Tier 1 to Tier 2).</p> 

Figure 45: Continuous Monitoring Wizard

Scoring Methodology

Firstly, it is important to note that not all of the requirements outlined by the CSF can be addressed fully by any single automated solution as certain aspects of the requirements may require people, procedural or operational processes to be implemented by an organization. There may also be requirements (Access Control, Training, Data Protection At-rest and In-Transit, etc.) that are not applicable to a specific group of applications such as GRC or human resources automated solutions. Accordingly, the analysis considers the requirements within the context of GRC product group such as TrustedAgent, and scores the requirements as follow:

1. If the requirement is clearly not applicable to the GRC solution category, the count of 1 is utilized for the requirement toward the number of NA Requirements.
2. If the requirement is fully addressable by the GRC solution, the count of 1 is utilized for the requirement toward the number of requirements met. The requirement can only be considered fully addressable when all of its sub-requirements are met.
3. If the requirement is only partially addressable or managed by the GRC solution, a count of 0.5 is utilized. Accordingly, if the requirement is applicable but is not met, a count of 0 is utilized.

Two scores are derived for each of the categories of the functions:

- a. Score A – Represents the percentage of the points obtained for the category across all possible requirements of that category. This score does not exclude requirements flagged as NA, and therefore is not a good indicator of how GRC solutions support CSF.
- b. Score B – Represents the percentage of the points obtained while excluding any NA, thus is more representative of the overall support percentage expected with a GRC solution.

TrustedAgent addresses the majority of the requirements outlined for the five functions of NIST CSF as indicated in the summary shown. For Identify Function, TrustedAgent offers strong support by providing asset management, governance, and risk management framework and assessment methodology. TrustedAgent also provides risk and incident management, detection and response, analysis, and remediation capabilities to address the Detect and Response Functions. Lastly, TrustedAgent supports the recovery activities from adverse events through policy management, updates, and reporting. Overall, TrustedAgent reduces the overall activities for an organization to cost-effectively and efficiently implement the requirements of CSF.

ALL FUNCTIONS				SCORE A	SCORE B
IDENTIFY [ID]				98%	98%
Asset Management (AM)	6.0		6	100%	100%
Business Environment (BE)	5.0		5	100%	100%
Governance (GV)	4.0		4	100%	100%
Risk Assessment (RA)	5.5		6	92%	92%
Risk Management (RM)	3.0		3	100%	100%
PROTECT [PR]				39%	80%
Access Control (AC)		5.0	5		
Awareness and Training (AT)	2.5		5	50%	50%
Data Security (DS)	2.0	5.0	7	29%	100%
Information Protection Processes and Procedures (IP)	4.5	7.0	12	38%	90%
Maintenance (MA)		2.0	2		
Protective Technology (PT)		4.0	4		
DETECT [DE]				68%	93%
Anomalies and Events (AE)	4.5		5	90%	90%
Security Continuous Monitoring (CM)	2.0	6.0	8	25%	100%
Detection Processes (DP)	4.5		5	90%	90%
RESPONSE [RS]				75%	80%
Response Planning (RP)	0.5		1	50%	50%
Communications (CO)	2.5		5	50%	50%
Analysis (AN)	3.0	1.0	4	75%	100%
Mitigation (MI)	3.0		3	100%	100%
Improvements (IM)	2.0		2	100%	100%
RECOVER [RC]				100%	100%
Recovery Planning (RP)		1.0	1		
Improvements (IM)	2.0		2	100%	100%
Communications (CO)		3.0	3		
Average across All Five Functions				75%	89%

Conclusion

NIST cybersecurity framework offers the sixteen critical infrastructure sectors a foundational framework that can be rapidly leveraged to enhance cybersecurity management for an organization. The approach is highly flexible and scalable and may be applied to organizations of different levels of cybersecurity maturity. For certain sectors, including oil and gas, electric, or water, and financial services, the framework has already demonstrated acceptance having been incorporated as sector-specific cybersecurity frameworks.

Voluntary adoption of the cybersecurity framework by organizations demonstrates 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 cybersecurity operations and activities to product time and cost savings also exist. Organizations stand to gain greater peer and customer recognitions and opportunities to command higher premium for the organizations' product and services.

Other collateral benefits such as lower cyberinsurance premium and lesser likelihood of regulatory and industry audits may also follow. An Enterprise Risk Management (ERM) approach for an organization would be incomplete if the organization fails to incorporate NIST cybersecurity framework as one of its core practices.

Governance, risk and compliance solutions such as TrustedAgent GRC can accelerate and strengthen the implementation of an effective cybersecurity program by automating or addressing many of the practices required by the framework. Furthermore, the right GRC solution such as TrustedAgent extends the benefits beyond initial implementation into ongoing monitoring and enhancement of security posture as maturity of the organization improves.

Appendix A – IDENTIFY Function Detailed Mapping to TrustedAgent

SUBCATEGORY	How TrustedAgent Supports Compliance
Asset Management	
ID.AM-1: Physical devices and systems within the organization are inventoried [Fully]	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.
ID.AM-2: Software platforms and applications within the organization are inventoried [Fully]	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. Examples of items are: <ul style="list-style-type: none"> Hardware items may include switches, routers, servers, firewalls, IPS and IDS, embedded controllers, PLCs, etc. Software items may include firmware, operating systems, applications, databases, etc.
ID.AM-3: Organizational communication and data flows are mapped [Fully]	TrustedAgent enables organizations to centrally manage key images and documents representing architecture and network diagrams, boundaries, workflows, interconnections, etc., and re-use across a number of key regulatory documents.
ID.AM-4: External information systems are catalogued [Fully]	Interconnections between information systems within the organization and to external entities outside of the organization can be managed along with characteristics of the information exchange, security and service level agreements, key contacts, and the authorization of the interconnections.
ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on the classification, criticality, and business value [Fully]	Resources (i.e., people, hardware, software, process, etc.) 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 be classified as a critical asset, or financial or privacy sensitive to highlight business value to the organization. An aggregated risk score of vulnerabilities associated with an asset can be leveraged to prioritize remediation efforts.

SUBCATEGORY	How TrustedAgent Supports Compliance
ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established [Fully]	TrustedAgent offers several built-in roles to support key workforce member assignment as well as custom roles defined by the organization. Standardizing roles ensure a clear assignment of roles for the workforce members in supporting authorization, maintenance, and incident response management. Suppliers, vendors, partners and customers can be tracked and managed as entities within TrustedAgent.
Business Environment	
ID.BE-1: The organization's role in the supply chain and is identified and communicated [Fully]	TrustedAgent allows organizations to manage their suppliers and vendors as entities. Information exchange and logistics between the organization and its suppliers can be managed through interconnections. Audits and vendor risk assessments to identify and understand the risk and ongoing remediation can be performed to monitor supplier compliance and performance to safeguard the supply chain.
ID.BE-2: The organization's place in critical infrastructure and their industry ecosystem is identified and communicated [Fully]	TrustedAgent utilizes a common descriptive framework to describe cybersecurity 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.
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated [Fully]	Organizations can prioritize (or categorize) entities based the risk rating using standard methods including NIST 800-60, 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. Custom data fields can be used by the organization to track additional information to further describe the priorities and criticality of entities within the organization.
ID.BE-4: Dependencies and critical functions for delivery of critical services are established [Fully]	Critical entities and relationship to other entities can be defined using a parent/child or program or site relationship. Key diagrams can be incorporated in to regulatory/industry reports. Interconnections can be created to define information sharing and business relationships between entities. Common controls can be established to promote critical functions and services provided across the organization.

SUBCATEGORY	How TrustedAgent Supports Compliance
ID.BE-5: Resilience requirements to support delivery of critical services are established [Fully]	For each of the organization's entities, contingency plan can be implemented and refined to meet specific resiliency requirements for the entity. The contingency plan may be maintained with relevant performance metrics (expiration and test dates, status, supporting artifacts). Resiliency requirements can be added to compliance requirements of critical services providers and assessed periodically for effectiveness.
Governance	
ID.GV-1: Organizational information security policy is established [Fully]	TrustedAgent provides a repository of policies that users can leverage and customize for their organization. Additional policies can be created and published to track adherence of the policies by end-users.
ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners [Fully]	User roles and responsibilities can be associated with established policies in TrustedAgent which can then be published to user to track adherence of the policies by users with the assigned role and responsibilities.
ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed [Fully]	TrustedAgent offers a large collection of open-source and commercial regulatory and industry standards to accelerate and maintain cybersecurity, regulatory or industry compliance program including NIST 800-53, ISO 27001, HIPAA, PCI, CIP5 and FFIEC.
ID.GV-4: Governance and risk management processes address cybersecurity risks [Fully]	Adoption of TrustedAgent demonstrates the organization's commitment to address cybersecurity practices. TrustedAgent supports a variety of risk management frameworks including NIST Risk Management Framework, Cybersecurity Framework, ISACA COBIT, ISO 27001, DIACAP, NERC CIP and others. The adopted frameworks can be integrated into both regulatory documentation and control content of the organization.

SUBCATEGORY	How TrustedAgent Supports Compliance
Risk Assessment	
ID.RA-1: Asset vulnerabilities are identified and documented [Fully]	TrustedAgent offers integrated vulnerability assessment (VA) tools to scheduling and conduct scans on demand or as scheduled 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 (configuration mapping file). Currently, XML connectors are supported for Nessus, AppScan, NetExpose, AppDetctive, Retina, and Rapid7.
ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources [Partially]	TrustedAgent supports sharing of incident reports to industry members and regulatory agencies. TrustedAgent interfaces with NIST National Vulnerability Database (NVD) and CPE databases to ensure that impacted assets and their CVEs can be quickly identified and remediated.
ID.RA-3: Threats, both internal and external, are identified and documented [Fully]	TrustedAgent supports threat assessment of assets through integrated and supported VA tools. Self-assessments and audits can also be conducted qualitatively using provided regulatory requirements or content provided with the selected risk management framework of the organization.
ID.RA-4: Potential business impacts and likelihoods are identified [Fully]	Identified findings are comprehensively supported with business impact analysis and recommended remediation action along with the assigned risk exposure level based on likelihood and impact levels.
ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk [Fully]	TrustedAgent supports complete life cycle management of findings and corrective actions (i.e., unlinked, active, in-progress, delayed, completed, etc.). Once identified risk can be categorized by likelihood, impact, and risk level. Corrective actions with appropriate risk level can be created to manage the remediation of risks.
ID.RA-6: Risk responses are identified and prioritized [Fully]	TrustedAgent's dashboard also provides real-time updates to findings and corrective actions as status of the risks and their remediation progress change. The dashboard is filterable and drillable to smaller organizational units and entity.
Risk Management	

SUBCATEGORY	How TrustedAgent Supports Compliance
ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders [Fully]	TrustedAgent platform serves as a technology platform to support the organization's risk management processes and related activities. Within TrustedAgent, organizations gain visibility and accountability to the risks of their entities, assets, and business processes and consistent approach to remediate and mitigate the risks.
ID.RM-2: Organizational risk tolerance is determined and clearly expressed [Fully]	TrustedAgent's template authoring allows the organization to define or revise controls associated with the selected framework with organization-specific requirements, response/implementation standards, and best practices.
ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis [Fully]	TrustedAgent enables risk tolerance to be defined at control level and be based on specific control templates defined to the CI sector. Risk tolerance may also be impacted based by the cybersecurity maturity of the organization. By default the control templates deployed are preset with risk levels commensurate to the CI sector. The control's risk level, if required, can be updated to match other values for other CI sectors.

Appendix B – PROTECT Function Detailed Mapping to TrustedAgent

SUBCATEGORY	How TrustedAgent Supports Compliance
Access Control	
PR.AC-1: Identities and credentials are managed for authorized devices and users	This requirement is applicable to the entities and the assets managed by the organization, and not directly to TrustedAgent.
PR.AC-2: Physical access to assets is managed and protected	This requirement is applicable to the entities and the assets managed by the organization, and not directly to TrustedAgent.
PR.AC-3: Remote access is managed	This requirement is applicable to the entities and the assets managed by the organization, and not directly to TrustedAgent.
PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	This requirement is applicable to the entities and the assets managed by the organization, and not directly to TrustedAgent.
PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	This requirement is applicable to the entities and the assets managed by the organization, and not directly to TrustedAgent.
Awareness and Training	
PR.AT-1: General users are informed and trained [Partially]	Policies and procedures can be developed and distributed to end-user using the policy management module. TrustedAgent also supports user acceptance and rejection of any published policies and procedures, to ensure users are trained to specific policies and procedures based on user role and responsibilities. Subsequently, audit reports can be obtained to indicate and confirm acceptance. An initial repository of policies is provided by TrustedAgent that can be customized and tailored by the organization.
PR.AT-2: Privileged users understand roles & responsibilities [Partially]	

SUBCATEGORY	How TrustedAgent Supports Compliance
PR.AT-3: Third-party stakeholders (suppliers, customers, partners) understand roles & responsibilities [Partially]	
PR.AT-4: Senior executives understand roles & responsibilities [Partially]	
PR.AT-5: Physical and information security personnel understand roles & responsibilities [Partially]	
Data Security	
PR.DS-1: Data-at-rest is protected	This requirement is applicable to the entities and the assets managed by the organization, and not directly to TrustedAgent.
PR.DS-2: Data-in-transit is protected	
PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition [Fully]	Assets associated with an entity can be updated or removed directly using TrustedAgent’s asset management module, or be modified using Excel data template import, or be updated through supported vulnerability assessment tools. Findings or vulnerabilities associated with any removed asset may either require justification to close, or be transferred (assigned) to the replacement asset to provide the regulatory evidence to demonstrate ongoing compliance. SDLC status can be assigned to entities allowing the entities to be managed accordingly to their lifecycle. For entities that are no longer in use (e.g., with SDLC of disposal), they can be filtered from the dashboard views allowing the key metrics to be updated to exclude these entities and the related assets.
PR.DS-7: Unnecessary assets are eliminated [Fully]	

SUBCATEGORY	How TrustedAgent Supports Compliance
PR.DS-4: Adequate capacity to ensure availability is maintained.	This requirement is applicable to the entities and the assets managed by the organization, and not directly to TrustedAgent.
PR.DS-5: Protections against data leaks are implemented	This requirement is applicable to the entities and the assets managed by the organization, and not directly to TrustedAgent.
PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	This requirement is applicable to the entities and the assets managed by the organization, and not directly to TrustedAgent.
Information Protection Processes and Procedures	
PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained [Partially]	TrustedAgent supports security categorization of entities to establish baseline controls to match the risk or maturity of the organization to support the requirements of the cybersecurity framework. Categorization also enables organizations to enforce consistency in ensuring baseline configuration is maintained and assessed. TrustedAgent also enables baseline configuration of assets (hardware, operating system, applications, etc.) associated to an entity to be maintained as artifacts. The artifacts can be scheduled for periodic verification of accuracy and completeness.
PR.IP-2: A System Development Life Cycle to manage systems is implemented [Fully]	TrustedAgent supports entities through the assigned SDLC life cycle. SDLC status can be leveraged to filter reports and dashboard views.
PR.IP-3: Configuration change control processes are in place [Partially]	This requirement is applicable to the entities and the assets managed by the organization, and not directly to TrustedAgent. However, TrustedAgent does provide a change management policy that can be leveraged and customized by the organization.
PR.IP-4: Backups of information are conducted, maintained, and tested periodically [Partially]	This requirement is applicable to the entities and the assets managed by the organization, and not directly to TrustedAgent. However, TrustedAgent supports the tracking of contingency plans developed and tested. TrustedAgent provides an initial contingency plan template that can leverage and customized by the organization.

SUBCATEGORY	How TrustedAgent Supports Compliance
PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met [Partially]	TrustedAgent provides a collection of physical and environmental policies that can be leverage and customized by the organization. Additionally, the tracking of compliance to physical and environmental policies and regulations can be managed as self-assessments and audits conducted by the organization.
PR.IP-6: Data is destroyed according to policy	This requirement is applicable to the entities and the assets managed by the organization, and not directly to TrustedAgent.
PR.IP-7: Protection processes are continuously improved	This requirement is applicable to the entities and the assets managed by the organization, and not directly to TrustedAgent.
PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	This requirement is applicable to the entities and the assets managed by the organization, and not directly to TrustedAgent.
PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed [Fully]	Out-of-the-box, TrustedAgent provides generic incident response and business continuity policies, procedures, and plans for organizations to leverage to ensure rapid implementation. TrustedAgent also supports customization of the documents for changes based on organization's requirements. The documents can be generated in real-time with key information maintained by the organization for the entities. Key performance metrics including status, scheduled completion date, and test date can also be tracked with the entity and the applicable document along with any supporting artifacts.
PR.IP-10: Response and recovery plans are tested [Partially]	TrustedAgent supports the development of the plans and the maintenance of performance metrics related to the testing of the plans. Findings are the results of the testing can also be managed within TrustedAgent.
PR.IP-11: Cybersecurity is included in human resources practices (de-provisioning, personnel screening, etc.)	This requirement is applicable to the entities and the assets managed by the organization, and not directly to TrustedAgent.

SUBCATEGORY	How TrustedAgent Supports Compliance
PR.IP-12: A vulnerability management plan is developed and implemented [Fully]	Similar to PR.IP-9, TrustedAgent's out-of-the-box deployment of CSF also contains a vulnerability management plan. Organizations can leverage TrustedAgent to further customize the plan based on organization's requirements. TrustedAgent also provides technical capabilities to further manage vulnerabilities in supporting the vulnerability management plan through integrated vulnerability assessment (VA) tools or through import XML results from VA tools.
Maintenance	
PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	This requirement is applicable to the entities and the assets managed by the organization, and not directly to TrustedAgent.
PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	This requirement is applicable to the entities and the assets managed by the organization, and not directly to TrustedAgent.
Protective Technology	
PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	This requirement is applicable to the entities and the assets managed by the organization, and not directly to TrustedAgent.
PR.PT-2: Removable media is protected and its use restricted according to policy	This requirement is applicable to the entities and the assets managed by the organization, and not directly to TrustedAgent.
PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	This requirement is applicable to the entities and the assets managed by the organization, and not directly to TrustedAgent.



SUBCATEGORY	How TrustedAgent Supports Compliance
PR.PT-4: Communications and control networks are protected	This requirement is applicable to the entities and the assets managed by the organization, and not directly to TrustedAgent.

Appendix C – DETECT Function Detailed Mapping to TrustedAgent

SUBCATEGORY	How TrustedAgent Supports Compliance
Anomalies and Events	
DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed [Fully]	TrustedAgent provides a common descriptive framework that establishes baseline configurations for information systems (ownership, characteristics, network/architecture diagrams, key contacts, risk or maturity rating, control requirements, authorization metrics, etc.) and system components (devices, applications, assets, parents) including communications (interconnections, cloud service and deployment type) and connectivity-related aspects of systems.
DE.AE-2: Detected events are analyzed to understand attack targets and methods [Fully]	When integrated or combined with supported vulnerability assessment (VA) scanning applications, TrustedAgent provides end-to-end management of entities and their assets of threat events and vulnerabilities ensuring ongoing remediation of vulnerable assets and reported incidents. TrustedAgent also supports continuous monitoring of key controls and scheduled/on-demand scanning of assets using supported VA tools.
DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors [Partially]	While this requirement is applicable to automated SIEM solutions such as intrusion detection and prevention technologies, TrustedAgent provides aggregation of identified risks against the impacted assets and the parent entities from several sources enabling organizations to understand the risk and compliance profiles of the entities and assets across the enterprise through its visual dashboard.
DE.AE-4: Impact of events is determined [Fully]	TrustedAgent's incident and finding management modules allow 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.

SUBCATEGORY	How TrustedAgent Supports Compliance
DE.AE-5: Incident alert thresholds are established [Fully]	Incident investigation details and business impact analysis, including threat types, likelihood, impact level, and resulting risk exposure level can be documented. One or more findings can be associated to finding reports as part of a continuous monitoring program, a specific security or privacy incident, or due to a specific external audit. Through risk mitigation discussion with entity's business owner and oversight staff, findings exceeding risk tolerance defined for the organization 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.
Security Continuous Monitoring	
DE.CM-1: The network is monitored to detect potential cybersecurity events [Fully]	TrustedAgent integrates with OpenVAS and SAINT vulnerability assessment scanners allowing scheduled scanning of assets for vulnerabilities, associated identified vulnerabilities to impacted assets, and creation of findings to ongoing remediation. XML results from other VA scanning tools can be filtered based on severity and imported into TrustedAgent for ongoing remediation.
DE.CM-8: Vulnerability assessments are performed [Fully]	
DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	This requirement is applicable to the entities and the assets managed by the organization, and not directly to TrustedAgent.
DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	This requirement is applicable to the entities and the assets managed by the organization, and not directly to TrustedAgent.
DE.CM-4: Malicious code is detected	This requirement is applicable to the entities and the assets managed by the organization, and not directly to TrustedAgent.
DE.CM-5: Unauthorized mobile code is detected	This requirement is applicable to the entities and the assets managed by the organization, and not directly to TrustedAgent.

SUBCATEGORY	How TrustedAgent Supports Compliance
DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	This requirement is applicable to the entities and the assets managed by the organization, and not directly to TrustedAgent.
DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	This requirement is applicable to the entities and the assets managed by the organization, and not directly to TrustedAgent.
Detection Processes	
DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability [Fully]	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.
DE.DP-2: Detection activities comply with all applicable requirements [Fully]	TrustedAgent supports VA scanning tools and non-technical assessments under a risk management framework, including NIST RMF, COBIT, or ISO. Risk and security rating can be performed using NIST 800-60, or PII. Privacy assessments can also be supported using NIST privacy or HIPAA controls using a privacy risk management framework consisting of privacy threshold analysis (PTA) and privacy impact assessment (PIA).
DE.DP-3: Detection processes are tested [Fully]	TrustedAgent provides a separate assessment view and user role enabling an assessor independent from the business owner to conduct verification of control implementation to determine control effectiveness. This process addresses conformity assessment approach recommended by NIST Cybersecurity framework and other risk management frameworks such as FFIEC (applicable to financial institutions), PCI, FedRAMP and ISO. For continuous monitoring, scheduled scanning of assets using integrated scanning tools can be performed on a periodic basis. Vulnerabilities identified can be reconciled against an entity and related assets for remediation.

SUBCATEGORY	How TrustedAgent Supports Compliance
<p>DE.DP-4: Event detection information is communicated to appropriate parties [Partially]</p>	<p>TrustedAgent comprehensively generates notifications (i.e., findings identified and corrective actions required) through emails and messageboard to responsible (assigned) users for changes to key data, activities coming due, delayed, etc. Additionally, users may employ alert filters to focus on notifications to specific statuses across the enterprise. Memo can also be communicated to entity owners for lessons learned or to communicate industry alerts.</p>
<p>DE.DP-5: Detection processes are continuously improved [Fully]</p>	<p>Integrated vulnerability assessment tools including OpenVAS and SAINT Scanner are periodically updated according to the vendor's specification from industry vulnerability feeds. TrustedAgent also integrates it CPE to NIST NVD and CPE Coupled with assessment support, TrustedAgent's dashboard and management reports provide the balanced scorecard information enabling organization to improve target profile to another maturity level (i.e., Tier 1 to Tier 2). Improvements and comparisons can be made across organization units based on similar metrics, specific to an entity, or aggregated across an enterprise.</p>

Appendix D – RESPONSE Function Detailed Mapping to TrustedAgent

SUBCATEGORY	How TrustedAgent Supports Compliance
Response Planning	
RS.RP-1: Response plan is executed during or after an event [Partially]	<p>TrustedAgent automates the development and maintenance of contingency plan and incident response plan, along with key supporting artifacts and performance metrics. Notifications are also available to ensure that the plans are periodically reviewed and maintained.</p> <p>TrustedAgent's finding and corrective action modules provides visibility to issues identified from the periodic testing of the response plans to ensure the plans are updated accordingly to minimize any identified gaps.</p>
Communications	
RS.CO-1: Personnel know their roles and order of operations when a response is needed [Partially]	In addition to the ability to document the responsible POCs for each entity, corrective actions and milestones can be assigned to one or more users. The assignment eliminates the need to rely on a person to collect the data and aggregate them for management reporting. In addition, organization gains visibility in improving resource planning as findings, corrective actions, and milestones are more visible outstanding to the organization by individuals.
RS.CO-2: Events are reported consistent with established criteria [Fully]	TrustedAgent enables the gathering of information consistent to industry requirements from US-CERT, HHS Breach Reporting, NERC/DOE, PCI and applicable industry standards or regulations to enable the incident response team to assess and report accordingly.
RS.CO-3: Information is shared consistent with response plans [Partially]	TrustedAgent's template authoring capability enables organization to construct and automate key reports to regulatory/industry bodies of security and privacy incidents and data breaches. The reports are can be based on industry and organizational requirements.

SUBCATEGORY	How TrustedAgent Supports Compliance
RS.CO-4: Coordination with stakeholders occurs consistent with response plans [Partially]	Key stakeholders can be managed as recipients of these documents improving communication and awareness of performance metrics and changes to the plans.
RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness [Partially]	By leveraging the template authoring module, organization can construct and deploy a standardized but redacted incident summary report for the sole purpose of sharing to external stakeholders.
Analysis	
RS.AN-1: Notifications from the detection system are investigated [Fully]	TrustedAgent's incident and finding management modules allow 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. Incoming incidents is queued for further review by an incident reviewer and handle accordingly.
RS.AN-2: The impact of the incident is understood [Fully]	Incident investigation details and business impact analysis, including threat types, likelihood, impact level, and resulting risk exposure level can be documented. One or more findings can be associated to finding reports as part of a continuous monitoring program, a specific security or privacy incident, or due to a specific external audit.
RS.AN-4: Incidents are classified consistent with response plans [Fully]	Through risk mitigation discussion with entity's business owner and oversight staff, incidents meeting organization requirements or/and exceeding the risk tolerance defined for the organization can be accepted for remediation. The remaining findings (with risk level below organization's risk tolerance) can be risk-accepted and rejected through justifications.
RS.AN-3: Forensics are performed	This requirement is applicable to the entities and the assets managed by the organization, and not directly to TrustedAgent.
Mitigation	
RS.MI-1: Incidents are contained [Fully]	In addition to the incident handling capabilities discussed using the incident reporting and finding management muddles, TrustedAgent provides a Memo-based approach for the

SUBCATEGORY	How TrustedAgent Supports Compliance
RS.MI-2: Incidents are mitigated	communication of lessons learned or industry notifications to end-users of external and internal incidents.
RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks [Fully]	<p>TrustedAgent integrates with OpenVAS and SAINT vulnerability assessment scanners allowing scheduled scanning of assets for vulnerabilities, associated identified vulnerabilities to impacted assets, and creation of findings to ongoing remediation. XML results from other VA scanning tools can be filtered based on severity and imported into TrustedAgent for ongoing remediation.</p> <p>Through risk mitigation discussion with entity's business owner and oversight staff, vulnerabilities meeting organization requirements or/and exceeding the risk tolerance defined for the organization can be accepted for remediation. The remaining findings (with risk level below organization's risk tolerance) can be risk-accepted and rejected through justifications.</p>
Improvements	
RS.IM-1: Response plans incorporate lessons learned [Fully]	TrustedAgent supports memo publishing to communicate lessons learned to personnel across the organization. Centrally managed policies and procedures can also be updated to incorporate or update activities from key learning points and disseminate to organizational staff. Once published, the acknowledgement of adherence for end-users can also be tracked.
RS.IM-2: Response strategies are updated [Fully]	Similarly, control requirements and best practices can also be updated using content authoring module enabling adoption of revised implementation standards and instructions incorporating response updates.

Appendix E – RECOVER Function Detailed Mapping to TrustedAgent

SUBCATEGORY	How TrustedAgent Supports Compliance
Recovery Planning	
RC.RP-1: Recovery plan is executed	This requirement is applicable to the entities and the assets managed by the organization, and not directly to TrustedAgent.
Improvements	
RC.IM-1: Recovery plans incorporate lessons learned [Fully]	TrustedAgent supports memo publishing to communicate lessons learned to personnel across the organization. Centrally managed policies and procedures can also be updated to incorporate or update activities from key learning points and disseminate to organizational staff. Once published, the acknowledgement of adherence for end-users can also be tracked.
RC.IM-2: Recovery strategy is updated [Fully]	Similarly, control requirements and best practices can also be updated using content authoring module enabling adoption of revised implementation standards and instructions incorporating response updates.
Communications	
RC.CO-1: Public Relations are managed	This requirement is applicable to the entities and the assets managed by the organization, and not directly to TrustedAgent.
RC.CO-2: Reputation after an event is repaired	This requirement is applicable to the entities and the assets managed by the organization, and not directly to TrustedAgent.
RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	This requirement is applicable to the entities and the assets managed by the organization, and not directly to TrustedAgent.

Trusted Integration is a boutique provider of Governance, Risk and Compliance (GRC) management solutions for highly-regulated government and commercial organizations. Our flagship product, TrustedAgent GRC, 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.

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