

SECURITY AUTHORIZATION OF HEALTH INSURANCE EXCHANGES

This whitepaper describes the utilization of TrustedAgent GRC to address the security and privacy requirements of MARS-E for state-based health insurance exchanges established under the Affordable Care Act.

Trusted Integration, Inc.
525 Wythe Street
Alexandria, VA 22314
703-299-9171 Main
703-299-9172 Fax
www.trustedintegration.com

“**Affordable Care Act is key driver behind the establishment of several state health insurance exchanges and Federal Health Exchange.**”

The Affordable Care Act, or ACA, requires that all Americans purchase a private health care plan, get an exemption or pay a 1% - 2.5% of their taxable income or a set amount. Americans who cannot afford health insurance will most likely either qualify for Medicare, Medicaid, CHIP or get assistance in the form of tax credits or assistance with up-front costs through their State's Health Insurance Exchanges (HIXs). If the insurance is still unaffordable after assistance (costing more than 8% of the family total income) individuals may be exempt from the Individual Mandate.

ACA is the key driver behind the establishment of several state health insurance exchanges and Federal Health Exchange, many of which opened for business on January 1, 2014 to provide up to 29 million people with affordable health insurance by 2019. However, not all states have chosen to run their own exchanges, some states including Texas, Oklahoma, Arkansas and a few others have defaulted to the Federal Health Exchange, also known as Healthcare.gov.

Out the 50 states, territories, and district, state decisions for creating HIXs in 2014 are tallied as follow:

- Seventeen (17) state-based health exchanges
- Seven (7) partnership health exchanges, where the state runs certain functions allowing the states to make key decisions and tailor the marketplace to local needs and market conditions.
- Twenty-seven (27) states on federally-facilitated marketplace (e.g., Healthcare.gov)

The choice to pursue a state run health exchange must be Federally-approved, primarily by the Secretary of Health and Human Services (HHS) in order to obtain the funding. The funding ranges for HIXs can vary from mid \$35M to as high as +\$1B for the larger states such as California¹. The state run HIXs will vary from state to state due to the flexibility offered by the ACA. State run HIX offers the state the maximum control and leeway as to how they will implement the exchanges.

¹ The Henry J. Kaiser Family Foundation, “State Health Facts”, <http://kff.org/health-reform/state-indicator/total-exchange-grants/#table>

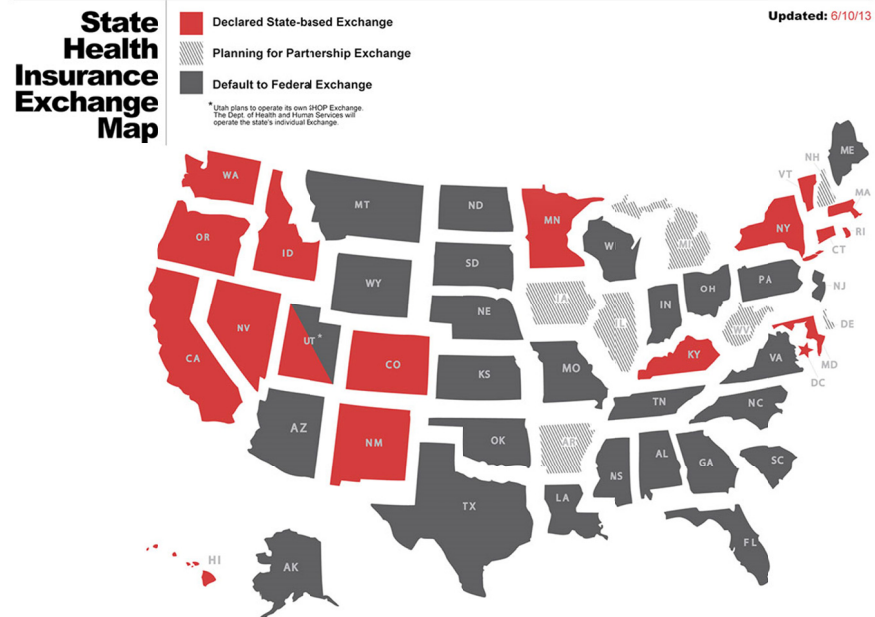


Figure A: State HIX Map²

Most exchanges are setup as non-profit, quasi-government corporations. Management structure of the HIXs also varies from state to state, but typically consists of an oversight community board and a day-to-day management team.

Security Authorization of Health Exchanges

One key aspect of data gathered by the state HIXs is the collection of the insurers' personally identifiable information (PII), protected health information (PHI), and Federal Tax Information (FTI). As the results, these HIXs are required to meet various security and privacy laws, statutes, and regulation from both federal as well as state sources and to undergo formal security authorization prior being placed into operational state. The primary requirements for the HIXs are established in the Minimum Acceptable Risk Standards for Exchanges (MARS-E) as published by the Centers for Medicare and Medicaid Services (CMS). MARS-E v1.0 is based on NIST SP 800-53 v3 with additional controls of IRS Pub 1075 to address the handling of IRS Federal Tax Information (FTI). In addition to HIXs, MARS-E is also applicable to a state Medicaid Agency, state Children's Health Insurance Program (CHIP), or a state basic health program (BHP).

² ObamacareFacts.com, "State Health Insurance Exchange Map", <http://obamacarefacts.com/state-health-insurance-exchange.php>

Challenges of Security Authorization Activities:

- **Complex**
- **Costly**
- **Time-consuming**
- **Error-prone**

Security authorization is a complex and time-consuming process that must be met by state or Federal government agencies for their IT systems, or by organizations that provide IT systems to state or Federal government agencies. Security authorization also requires expertise that is both costly and hard to find in today's competitive cybersecurity marketplace. Regulations are increasingly becoming more complex, placing greater demands on organizations to demonstrate with substantial evidence of their compliance. Compliance is no longer an option, but is becoming a business necessity with governing agencies issuing massive multiple hundreds of thousands to millions of dollars in penalties for noncompliance.

Requirements of MARS-E

MARS-E provides the security and privacy standards from which exchanges are required to follow to address the requirements of HHS Final Rule on ACA Exchanges, Section 155.260, and CMS is tasked with the oversight responsibilities for establishing the standards and their HIX implementation. Each health exchange requires to conduct review of their HIX IT systems using the MARS-E standards, and to issue a formal security authorization prior to granting an Authority-to-Operate (ATO).

MARS-E sets the minimum security and privacy requirements to be applied against IT systems supporting HIXs under ACA. HIX must clearly define the infrastructures and systems that support the HIX, document the implemented controls, maintain supporting evidence, and conduct security assessment to confirm the effectiveness of the controls. It is important to note that, unlike security authorization process under Federal Information Security Management Act (FISMA) applicable to Federal IT systems where multiple security categorization levels may exist, most HIXs are categorized as Moderate. Another similarity to FISMA is the use of third-party security assessment to review the effectiveness of control implementation. Granted that the cost may be more or less depending on the technical architecture and compliance maturity of the exchange, the cost of reviews was found to vary from low \$45k³ to \$1.2M⁴ based on our research.

³ Maryland State Health Exchange Procurement, "Cost of Third-Party Security Assessment for Maryland State Health Exchange", <http://marylandhbe.com/news-and-updates/procurement/>

Control Families in MARS-E

- Access Control (AC)
- Awareness and Training (AT)
- Audit and Accountability (AU)
- Security Assessment and
- Authorization (CA)
- Configuration Management (CM)
- Contingency Planning (CP)
- Identification and Authentication (IA)
- Incident Response (IR)
- Maintenance (MA)
- Media Protection (MP)
- Physical and Environmental Protection (PE)
- Planning (PL)
- Personnel Security (PS)
- Risk Assessment (RA)
- System and Services Acquisition (SA)
- System and Communications Protection (SC)
- System and Information Integrity (SI)
- Program Management (PM)
- FTI Safeguards

The number of control families covered by MARS-E is similar to the 18 families of NIST 800-Rev 3 with the addition of three additional controls under one unique IRS family. The controls for the most parts share significant similarity to the NIST 800-53 controls, with exception of the addition of Implementation Standards, where key parameters, frequencies, or any other additional or unique requirements are clear specified for the control or control enhancement for the exchanges. Another key difference between the MARS-E vs. NIST controls is the inclusion of FTI specific requirements from IRS-1075 publication as part of the Implementation Standards.

TrustedAgent GRC and Compliance of Health Exchanges

By leveraging automated governance, risk and compliance (GRC) solutions such as TrustedAgent GRC, the processes and activities supporting security authorization of a health exchange under MARS-E standards are significantly simplified resulting in a timely, error-free implementation, and cost-effective approach. Out-of-the-box GRC solutions deliver one or more standardized risk management frameworks and content (e.g., security control set, document templates, appendices, etc.) for the organization to meet the requirements of the governing regulations. For example, TrustedAgent defaults to the well-known security authorization process of NIST 800-37 Risk Management Framework (RMF); however, other frameworks such as COBIT, Cybersecurity Framework, or ISO 27001 can also be utilized.

In certain cases, some HIXs may also be required to follow the requirements of HIPAA/HITECH or other state-specific requirements. In either case, TrustedAgent offers HIPAA/HITECH content add-ins or the authoring module can be leveraged to add custom controls to address state-unique requirements.

TrustedAgent (TA) Risk Management and Compliance 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.

⁴ California Health Benefit Exchange, "Solicitation HBEX-8 – Visionary Integration Professionals", <https://www.coveredca.com/hbex/solicitations/>



Figure 1: NIST Risk Management Framework

- Define.** Entities such as information systems, security programs, data centers or vendors are managed within TrustedAgent. Entity characteristics, points of contact, interconnections, hardware and software assets, and architectural/design diagrams are recorded to support the authorization of the entity. Key requirements addressable for MARS-E by TrustedAgent are:

Requirements	Key Activity Supported by TrustedAgent
MARS-E establishes minimum security control guidance for all Exchange IT information systems for which CMS has oversight responsibility, starting with Exchanges and common program enrollment systems as required by the Affordable Care Act.	<ul style="list-style-type: none"> Identify Relevant Information Systems (that house or process Exchange-owned PII or PHI, Exchange IT systems, common program enrollment systems, Federal Tax Information (FTI) for the purpose of supporting Exchange). Inventory of authorized and unauthorized devices Inventory of authorized and unauthorized software
§155.260 of the HHS Final Rule stipulates that Exchanges must require the same or more stringent privacy and security standards as a condition of contract or agreement with individuals or entities, such as Navigators, agents, and brokers that have access to Exchange-owned PII.	The rules apply to all Exchange employees, contractors, subcontractors, and their respective facilities supporting such IT systems, or have access to Exchange-owned PII.
Identify data elements sourced from federal agencies for the identified inventory.	<ul style="list-style-type: none"> Document key attributes (i.e., name, purpose, location, ownership, etc.) for the applicable IT systems Identify personnel responsible for oversight, development, security, privacy, and support of the systems. Identify the business process (es) associated with the systems. Identify the system environment. Identify system interconnections. Identify the system security level. Identify the hardware (equipment or device) list. Identify the software utilized.

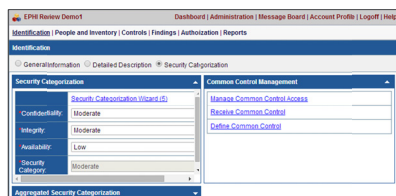


Figure 2: Security Categorization



ID	Name	Information Type	Name	Confidentiality	Integrity	Availability	Security Category
001	001.001	001.001	001.001	Low	Low	Low	Low
002	002.001	002.001	002.001	Low	Low	Low	Low
003	003.001	003.001	003.001	Low	Low	Low	Low
004	004.001	004.001	004.001	Low	Low	Low	Low
005	005.001	005.001	005.001	Low	Low	Low	Low
006	006.001	006.001	006.001	Low	Low	Low	Low
007	007.001	007.001	007.001	Low	Low	Low	Low
008	008.001	008.001	008.001	Low	Low	Low	Low
009	009.001	009.001	009.001	Low	Low	Low	Low
010	010.001	010.001	010.001	Low	Low	Low	Low

Figure 3: Categorization Wizard

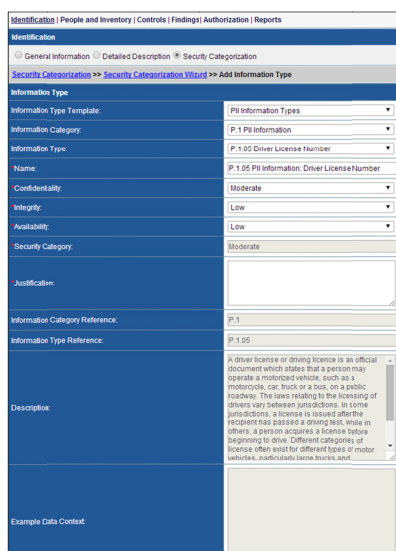


Figure 4: PII Categorization

Requirements	Key Activity Supported by TrustedAgent
Identify how security is addressed in all levels of development;	System development life cycle (SDLC) can be associated with any given entity allowing the security categorization to also be considered with regard to the SDLC status.

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. Under MARS-E, Exchange IT systems are classified as Moderate based on FIPS199 and contained PII, PHI or FTI.

Requirements	Key Activity Supported by TrustedAgent
Baseline controls define the control standards by control families to support the implementation of the critical technical, management, and operational controls needed to defend against the most common and damaging computer and/or network attacks.	Perform security categorization.
Security categorization using FIPS199	TrustedAgent's security categorization wizard automates the categorization process using the selected control template for the entity to determine the baseline controls.
Categorization using PII	TrustedAgent's security categorization wizard can also be leveraged to determine the extent in which PII are utilized or processed by the Exchange IT systems, and to adjust the baseline controls accordingly.

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. The Control Assessment Matrix is refined to exclude common controls and controls that are not applicable.

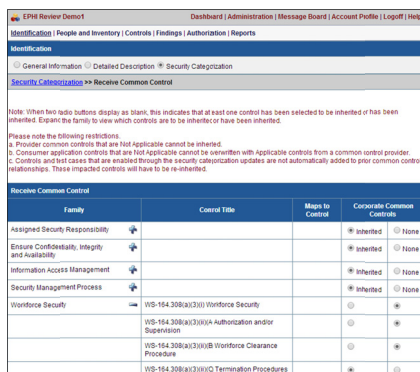


Figure 5: Common Control Management

Requirements	Key Activity Supported by TrustedAgent
In some cases, the Exchange system owner may implement the control on a parent system and have subordinate systems inherit the control from the parent system.	Common controls from one or more providers may be established using TrustedAgent common control framework. When inherited, the control's implementation and effectiveness as indicated by the associated test case results are taken from the provider saving significant time and improve consistency in ensuring control effectiveness.
An Exchange system owner may choose to strengthen the controls implementation beyond the defined requirements to provide additional protection of Exchange IT information and information systems.	Using the build-in control scoping capability, optional controls as defined as NIST can also be leveraged from the selected control template to provide additional safeguards to Exchange IT systems. Controls can be scoped upward or downward as to reflect the available safeguards to the systems.
Identify and provide details on the security controls related to the system within the NIST 800-53 (for moderate impact level), control families and those for FTI, if applicable;	This process is accomplished through the combination of the security categorization and control scoping.

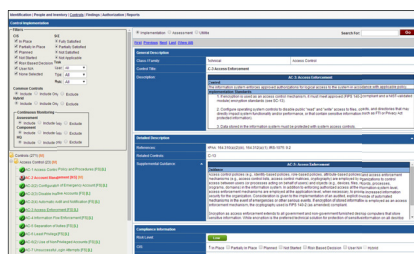


Figure 6: Control Implementation

Compliance Details						
Item	Item	Item	Item	Supporting Artifact	ES&M Validation	HQ Review
1	Authorization	Artifact	Artifact	Artifact	Artifact	Artifact
2	Supplement	Artifact	Artifact	Artifact	Artifact	Artifact

Figure 7: Artifacts for Control Implementation

- Implement.** The baseline controls are implemented and documented accordance with the applicable implementation standard. Some implementation standards may contain specific recommended definitions or event values (such as "90 days") as the compliance standard for a given control. Other implementation standards are based on specific types of data, such as PHI, PII, or FTI. TrustedAgent's MARS-E control template addresses seven key sections of control definition including Baseline and Implementation Standards, Enhancement Control, Guidance, Applicability, Reference, Related Control Requirements, and Assessment Procedure.

The control implementation status and compliance details including applicable artifacts are documented in the system security plan (SSP) based on the template defined by CMS to meet the requirements of

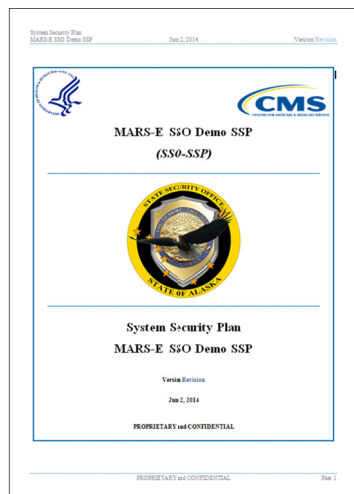


Figure 8: MARS-E SSP Sample

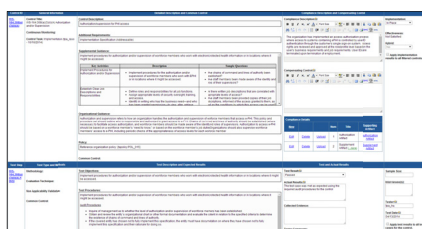


Figure 9: Security Control Assessment



Figure 10: Security Assessment Report

MARS-E security authorization process.

Requirements	Key Activity Supported by TrustedAgent
Create and Maintain System Security Plan	<ul style="list-style-type: none"> TrustedAgent automates the generation of SSP to document control implementation along with supporting information including, but not limited to: system details, boundaries, key architecture diagrams, categorization and use of common controls, asset information (hardware, software, and operating systems), etc. Changes to SSP are centrally managed in real-time saving significant time for updates due to changes and reduction in errors.

- Assess.** Controls are assessed by independent assessors using test procedures for MARS-E controls drawn from NIST 800-53A with modifications to address the specific Implementation Standards of the controls. During the security assessment process, where a control may not be fully satisfied, finding may be documented in the Security Assessment Report for later discussion with system owners.

Requirements	Key Activity Supported by TrustedAgent
Conduct Security Assessment	<ul style="list-style-type: none"> Assessors conduct review of controls implemented with provided test cases according to MARS-E requirements. Additional or custom test cases can also be added using the built-in content authoring capability.
Provide Security Assessment Report	<ul style="list-style-type: none"> Automates SAR based on the organization's template with the relevant details including the identification of effective and not effective (unsatisfactory) controls, and both summary and detail findings and their statuses to support an ATO. SAR template can be also modified as required to incorporate additional organization's specific requirements.

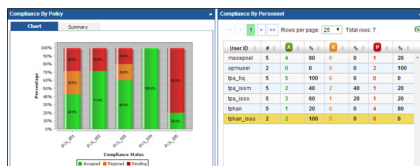


Figure 11: Policy Dashboard

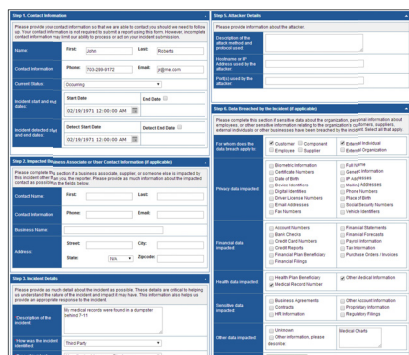


Figure 12: Incident Identification

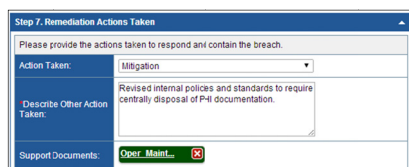


Figure 13: Incident Review & Analysis

Requirements	Key Activity Supported by TrustedAgent
Policy Management	<p>Organization policies and procedures can be centrally created, managed and communicated to end-users supporting incident response capability with the added benefits of supporting organization-wide policies and procedures.</p>
Incident Identification	<ul style="list-style-type: none"> Incidents are automatically and centrally managed as findings through an incident management program setup as an entity for managing incidents within TrustedAgent. Privacy and security incidents can be centrally collected from reporters consistent to recommended practices from NIST SP-800-61, US-CERT and HHS Incident Reporting. Information gathered include the reporter, involvement from any third-party vendor/business associates, type of the incident, impact to any specific organizational assets, devices, or system, methods of attack, and the extent of the incident and the type of data that was potentially compromised. Artifacts supporting incident identification can also be tracked.
Incident Review and Analysis	<ul style="list-style-type: none"> Incidents are reviewed by analysts per organization policies and procedures and disposition accordingly based on actions taken (risk remediated, reporting requirements, etc.). Findings generated for incidents are centrally managed preventing the possibility of overlooking an specific incident. Incidents meeting organization requirements can be linked to a corrective action plan (CAPs) and the CAP can be assigned to applicable entities for remediation.

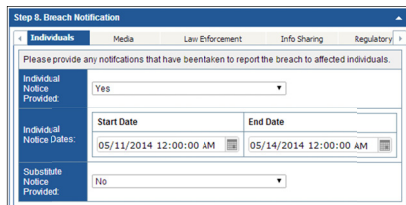


Figure 14: Incident Reporting

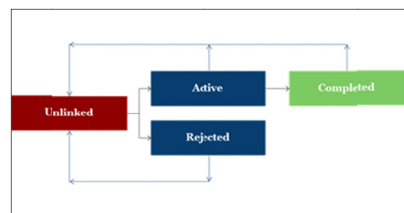


Figure 15: Lifecycle of Findings

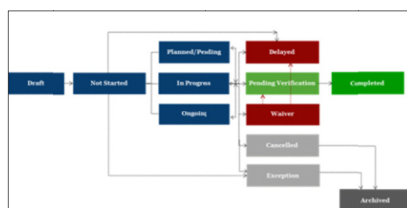


Figure 16: Lifecycle of CAPs



Figure 17: Finding Dashboard



Figure 18: CAP Dashboard

Requirements	Key Activity Supported by TrustedAgent
Incident Reporting	<ul style="list-style-type: none"> Incidents are reported to internal and external parties. Lesson learned can be updated into centrally managed incident response policies and procedures. Breach notification to impacted individuals, media, law enforcement, industry group, and internal management can be documented.

6. Manage. Findings identified from control implementation and assessment or from vulnerabilities scanning of assets can be managed for remediation through a defined life cycle framework. Corrective actions (CAPs), or remediation plans, may be generated for findings that are not Fully Satisfied and where risks have not been accepted by the authorizing official, or have legal or regulatory consequences if not addressed. Similarly findings, TrustedAgent offers a comprehensive defined life cycle framework for managing CAPs until closure.

Requirements	Key Activity Supported by TrustedAgent
Manage findings for mitigation or remediation.	<ul style="list-style-type: none"> Findings can be created and managed with life cycle as shown. Findings are linkable to failed control(s) or control test case(s). Findings can also be tracked to manage issues identified by external or regulatory auditor such as CMS OCR or OIG. Finding and corrective action dashboard views provide real-time visibility and accountability into findings, vulnerabilities, and corrective actions under remediation by status, risk level and by asset type.
Management of remediation plans for significant or material findings.	Formal remediation plan with multiple milestones can be created to manage findings from regulators.

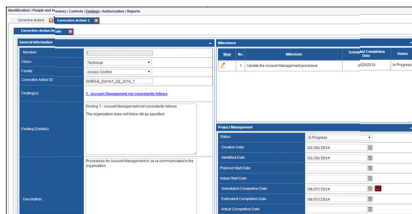


Figure 19: CAP Details

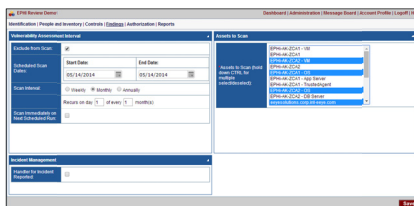


Figure 20: Integrated Vulnerability Management



Requirements	Key Activity Supported by TrustedAgent
Continuous vulnerability assessment and remediation	<ul style="list-style-type: none"> TrustedAgent integrates with industry vulnerability assessment scanners to enable the centrally management of vulnerabilities by assets across the enterprise. TrustedAgent supports the specification of key and standard controls required to be assessed for a given assessment period (calendar or fiscal year).
Penetration tests and red team exercises	<ul style="list-style-type: none"> TrustedAgent supports the penetration testing using industry tools such as Appscan or through manual technique. Findings from penetration testing can be managed as external audit reports to remediate the identified issues.

7. Authorize. The authorization package is presented to the authorizing official for review and approval. ATO 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 and incorporated into key documents.

Requirements	Key Activity Supported by TrustedAgent
System security plan (SSP) Safeguard Procedures Report (SPR) Workbook for SSP (SSP Workbook)	TrustedAgent automates the creation of the SSP along with the control compliance details, implementation status, control test results and the assessed control effectiveness. Compensated controls, if utilized, can also be included in the SSP.
Security Assessment Report	Automates the SAR with the relevant details including ineffective controls, both summary and detail findings, and their statuses to support an authorization decision.

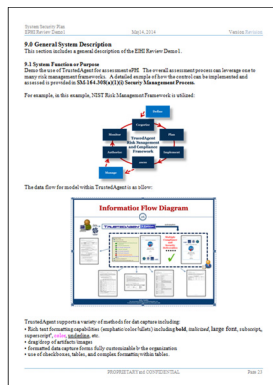


Figure 21: Content Authoring for SSP

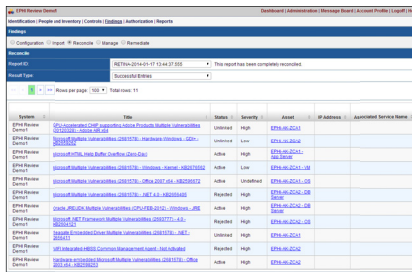


Figure 22: Automated Finding Reconciliation to Assets from Vulnerability Scans

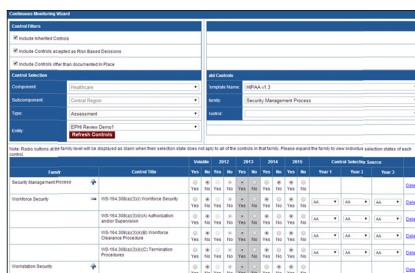


Figure 23: Continuous Monitoring Wizard

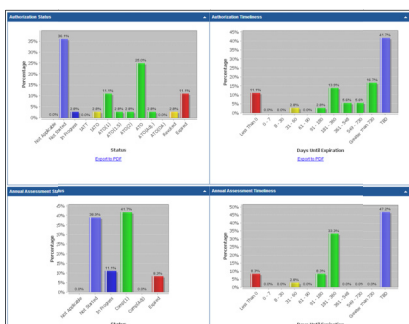
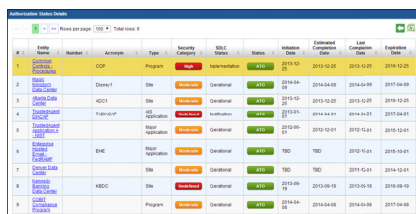


Figure 24: Authorization Dashboard

Requirements	Key Activity Supported by TrustedAgent
Executive Summary	The executive summary can be automated using the SAES template within TrustedAgent. The template can be further customized by the organization.
Content Template Authoring	Content authoring enables regulatory templates discussed above to be customized to create and incorporate organization-specific requirements.

8. Monitor. Ongoing security reviews, assessments, and remediation of findings, vulnerabilities and corrective actions are performed and tracked using management dashboard views, notifications, and reports. Periodic testing of assets for vulnerabilities using support vulnerability assessment scanning tools for regulatory monitoring, re-authorization, or due to significant change can also be managed. Where significant changes impact baseline controls, TrustedAgent supports the retesting of the controls, and automates the updated results across regulatory reports such as system security plan and assessment report.

Requirements	Key Activity Supported by TrustedAgent
Continuous vulnerability assessment and remediation	<ul style="list-style-type: none"> For supported applications including SAINT Scanner and OpenVAS TrustedAgent enables vulnerability assessment scans to be centrally managed, scheduled using a predetermined frequency, and identified findings are automatically reconciled to the assets and the entities. Supports the retesting of baseline controls for significant changes against assets of an entity. Key controls as mandated by organization or regulatory requirements can be evaluated as required.



ID	Name	Number	Activity	Type	Status	Milestone	Last Completion Date
1	Authorization	123456	Authorization	Program	Active	2015-10-01	2015-10-01
2	Authorization	123457	Authorization	Program	Active	2015-10-01	2015-10-01
3	Authorization	123458	Authorization	Program	Active	2015-10-01	2015-10-01
4	Authorization	123459	Authorization	Program	Active	2015-10-01	2015-10-01
5	Authorization	123460	Authorization	Program	Active	2015-10-01	2015-10-01
6	Authorization	123461	Authorization	Program	Active	2015-10-01	2015-10-01
7	Authorization	123462	Authorization	Program	Active	2015-10-01	2015-10-01
8	Authorization	123463	Authorization	Program	Active	2015-10-01	2015-10-01
9	Authorization	123464	Authorization	Program	Active	2015-10-01	2015-10-01

Figure 25: Authorization Details

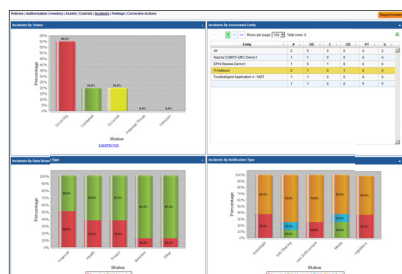


Figure 26: Incident/Breach Metrics



Alert Type	Status
Corrective Action Alert	<input checked="" type="checkbox"/>
Controls Alert	<input checked="" type="checkbox"/>
POC Alert	<input checked="" type="checkbox"/>
Entity Information Alert	<input checked="" type="checkbox"/>
Interconnection Alert	<input checked="" type="checkbox"/>
Activity Summary Alert	<input checked="" type="checkbox"/>
Quality Alert	<input checked="" type="checkbox"/>
Milestone Alert	<input checked="" type="checkbox"/>
Authorization Alert	<input checked="" type="checkbox"/>
User Access Alert	<input checked="" type="checkbox"/>
Finding Alert	<input checked="" type="checkbox"/>
Asset Inventory Alert	<input checked="" type="checkbox"/>
Change Summary Alert	<input checked="" type="checkbox"/>

Figure 27: Event-based Notifications

Requirements	Key Activity Supported by TrustedAgent
Management dashboard and reporting	<ul style="list-style-type: none"> TrustedAgent's dashboard views provide real-time access to several key performance metrics including authorization, entities, assets, findings and corrective actions to support authorization and continuous monitoring of risks across the organization. The metrics may be filtered by attributes related to the entities, by organizational hierarchy, or by other attributes as determined by the end users. Dashboard and other reporting features are available for users to filter controls required to be assessed based on their assigned continuous monitoring period and type.
Notifications	<ul style="list-style-type: none"> Event-based notifications enable end-users to receive timely notifications of activities coming due and in real-time for data changes meeting specific criteria specified by end-users.

TrustedAgent addresses the activities to meet the requirements specified by MARS-E, enabling the HIX owners to focus on the details that truly matters such as ensuring adequacy of security and privacy implementation and ongoing management of exchange operation. The benefit also extents to compliance management to come by enable the HIX's readiness to support expected future updates of the MARS-E control catalog. Continuous monitoring of controls for remediation and asset changes are also supported along with integration to vulnerability assessment tools allowing scan results to be imported for remediation.

Conclusion

Health exchanges must undergo security authorization using MARS-E standards established by CMS prior to granting an ATO as the health exchanges collect PII, PHI, and FTI data about individuals. The security authorization evaluates privacy and security practices of the HIX and the IT systems supporting the exchange.

GRC solutions, such as TrustedAgent GRC, can substantially reduce the effort required to support ongoing compliance management of the HIXs by automating multiple activities of the security authorization process. The use of GRC tools reduces the total cost of maintaining an exchange while enforcing a consistent and standard-based approach to privacy and security review. The tool drives cost reduction and efficiency by enabling HIX oversight staff to monitor compliance activities being performed by its contractors supporting the various aspects of the security authorization for the exchange.

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

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

Trusted Integration, Inc.
525 Wythe Street
Alexandria, VA 22314
703-299-9171 Main
703-299-9172 Fax
www.trustedintegration.com