Challenges of Security Authorization Activities:

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

TrustedAgent provides a comprehensive, enterprise platform that integrates, standardizes, and enhances the existing Governance, Risk and Compliance (GRC) processes, and enables organizations to meet the challenging, complex, and changing requirements of PCI, SOX, HIPAA, NERC, GLBA, MARS-E, FISMA, FedRAMP, and many others.

Security authorization is a complex and time-consuming process that must be met by government agencies for their IT systems, or by organizations that provide IT systems to 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.

A well-known security authorization process is the NIST 800-37 Risk Management Framework, from which TrustedAgent models its 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.

1. **Define.** Reportable and non-reportable entities are managed within TrustedAgent. Entity characteristics, points of contact, interconnections, hardware/software assets, and architectural/design diagrams are properly recorded to support the authorization of the entity. A System Information Profile (SIP) or other inventory profile documentation can be created as an outcome of this task.

2. **Categorize.** Security categorization processes are employed to determine applicable security requirements. A Control Assessment Matrix is created as an outcome of this task. Controls are defined based on predefined organizational templates that can be tailored across the various components and business units within the organization.

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 1: NIST Risk Management Framework

4. **Implement.** The controls are implemented and documented for compliance in accordance with organizational and regulatory requirements. System security plans, DIACAP Implementation Plan (DIP), or other organizational documents can be generated to report on control implementation status and compliance details.

5. **Assess.** Controls are assessed by independent assessors. Control Assessment Plan, Security Assessment Results (SAR), DIACAP Scorecard, 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.

6. **Manage.** Findings are 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. A Security Authorization Executive Summary (SAES) or other organizational document can be created from predefined templates to document the recommendation for the authorization of the entity.

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.

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.

Many organizations attempted to manage security authorization activities using existing technologies and people, referring to as *"the manual method"*, by leveraging information that may already exist in forms of spreadsheets, electronic documents (Word or PowerPoint), reports (printed

and scanned), images, other electronic data, etc., disparately locate across the enterprise. The more savvy organizations also attempted to overcome this disparate state of information by adopting a centralized approach to data management either through the use of enterprise collaboration tools such as Sharepoint, or through the use of shared folders within a network. These bits of information, or artifacts, serve as bodies of evidence to support a compliance position, or statement in the development of a compliance profile. This approach is not without critics due to the lack of assurance of data accuracy and integrity of the centrally managed information as the same data may be editable by multiple users, possibly without or limited use of audit trails or version control. Regardless of the methods taken, the manual method to security authorization delivers incrementally small successes as the manual process does not scale well beyond the three or four reportable systems mostly present within micro-agencies.

"The percentage shown represents the average amount of time saved to accomplish the outlined activity using TrustedAgent in comparison to the manual method."

TrustedAgent automates a large number of security authorization activities that would normally be prohibitively expensive to be manually implemented by the medium and large organizations. This case study compiles data from the various deployments of TrustedAgent (where authorized), time trials, and attempts to provide quantifiable savings that organizations can consider in making a case for acquiring an automated security authorization solution. Included in our benchmark is a major life science organization that contains several hundreds of reportable inventories well balance with a good mix of low, moderate, and high systems. The organization also employs common controls and control scoping in their implementation as well as conducting conformity assessment of applicable controls. The organization requires typical regulatory documents including risk assessment, security plan, business contingency plan, control test plan, control assessment report, and executive authorization summary.

Since the maturity and internal experience on security authorization process may vary from organization to organization, the data were normalized against the manual method established through time trials or customer interviews or combination thereof to derive the key metrics. The percentage shown represents the average amount of time saved to

accomplish the outlined activity using TrustedAgent in comparison to the manual method. Organizations can obtain the actual time savings from using TrustedAgent by multiplying the percentage shown by the actual time required to perform the same task for the organization.

DEFINE Phase

Content Management	90% Reduction

For any given week, conservatively, the compliance staff will likely to spend about 2 hours updating policies and procedures, control templates, and other regulatory documents ensure ongoing compliance to the latest regulatory rules[1]. Updates are necessary activities as compliance documents must reflect current regulatory standards to ensure accurate control implementation, assessment and authorization decisions.

- Out of the box TA provides with rich text security authorization templates that meet the regulatory requirements and easily customizable to organization' specifications.
- By centrally maintain the templates within TrustedAgent, changes to the master templates can be quickly updated, thereby eliminates duplication of editing and errors relating to change management across the organization.
- The templates are re-useable to other components or subcomponents within an organization to enforce consistency and compliant to policies/procedures.
- Security templates such NIST 800-53, HIPAA, or FedRAMP are presented as provided from primary sources, eliminating the need to document control objective, guidance, test cases, test procedures, etc.
- Change from one revision of control template (e.g. NIST 800-53 Rev 3 to Rev 4) can be facilitated within few minutes compared to hours as manual method, substantially reduce the cost of maintenance as new controls are implemented or updates.
- Implementation of organization wide guidance or best practices can be incorporated into TA control template and disseminate to all systems.
- Customized responses to specific controls can be facilitated for any given control, thereby ensure consistency in data capture across organization's inventory.

[1] "Cost of Compliance Survey 2013", Thomson Reuters, 2013

- TA provides built-in support to author and update content; thereby organizations can rapidly implement changes or add new templates to meet changing or new regulations.

Inventory and Asset Management	66% Reduction

For most organizations, included those benchmarked by Trusted Integration, inventory and asset information tends to remain unchanged requiring very limited update on the behalf of the business owner. The number of assets requiring update does not play a significant role in impacting the time requirements due to the availability of asset management tools to output the data into forms that can be managed by an automated security authorization tool. In our benchmarking at a major organization with an inventory of several hundred systems, we derived an average time to update inventory and asset management per system to be approximately 102 hours per year.

- Data templates are available to load key information to migrate existing systems into TA, accelerating data setup and updates.
- Assets (hardware/software) associated with an inventory system can be updated using data templates or from vulnerability assessment results such as Nessus. CPE information is automatically matched to asset using lookups to NIST NVD.

CATEGORIZE Phase

Security Categorization	95% Reduction

All automated security authorization automates the security categorization using either PII or information types, or both, based on NIST 800-60. In our benchmark, the time estimated is merged with the baseline selection, and collectively it was calculated to be about 4 hours per control per year.

- TrustedAgent automates FIPS 199 process from the information types provided for the systems including category, information, default category/information type descriptions from NIST 800-60, and default impact levels (CIA).
- TA enables organization to categorize their PII as well as to leverage their own FIPS process.
- TA automates the determination of overall security categorization based on individual confidentiality, integrity, and availability.

PLAN Phase

Common Controls	94% Reduction

Our benchmark reveals that the common controls are setup for initial implementation based on the organization's common controls program. The subset of the common controls, approximately a third, is revisited on annual basis for re-update using an approach similar to that of continuous monitoring. The cost per common controls per update per year is two hours and is not significant when compared to other costs.

- TrustedAgent facilitates the capabilities to define and document common controls for one or more provider system(s). The captured information can be inherited into SSP of consumer systems. Having these capabilities are significant time savings as, for example, NIST 800-53 Rev 3, typical setup has about 122 common controls.
- TA automates the control implementation and assessment, as well as control documentation for common controls in the consumer systems from one or more providers. This is a significant time savings as more provider sources are added, the time required for documenting common controls in consumers increases.

Baseline Control Selection	95% Reduction

Refer to Categorize Phase for a discussion on the benchmark related to baseline control selection.

- TrustedAgent automates the tedious and error-prone process of identify and document the applicable baseline controls using the overall security category defined for the system. For example, a moderate system requires a selection of 170 controls vs. a low system of 123 controls, excluding any common controls. The larger the control sets the more time consuming the process to be performed manually as seen with NIST 800-53 Rev 4 where the control enhancements are broken out as standalone controls.
- TA facilitates updates for control scoping if scoping is allow the organization. Scoping is very uncommon, and is estimated at 1% of any given control set. Re-scoping impact applicable test case and assessment testing, and therefore the process is very error prone.

IMPLEMENT Phase

Control Implementation	60% Reduction

The determination of the control implementation time requirement proves challenging as controls are implemented over time. Metrics were obtained from a combination of interviews with clients and from literature search[2]. The general consensus of the data reviewed indicates that control implementation typically requires approximately 18 hours per control per year. It is also interesting to note that, in at least one security plan reviewed, five controls were annotated as not applicable to the baseline when the controls are applicable. This error represents 3.4% of the controls population, thus one would expect that the time required for control implementation and assessment to be adjusted higher by the error rate shown.

- TrustedAgent methodically assists the system owner to document control implementation status and compliance description for the assigned systems. TA has built-in event-based workflows to manage the multiple priorities; distractions, etc. typically found in most organizations, allowing system owner to gain timely control implementation and to reduce delays impacting control implementation.
- TA provides ability to distribute the control implementation and assessment across a team of users while allowing organization oversight staff to gain visibility to control implementation. By eliminate the 'middleman', this approach accelerates implementation and reduces potential errors of having to aggregate and document information from multiple parties.

ASSESS Phase

Control Implementation	60% Reduction

Using the same technique described for control implementation, the assessment time requirement in manual method was calculated to be 26 hours per control per year. The additional hours accounted for the review of the artifacts submitted by the business owner for the implemented control and the number of applicable test cases to be assessed.

[2] "A framework for Estimating ROI of Automated Internal Controls", ISACA, 2011

- TrustedAgent accelerates control testing and related documentation. Assessment analysts can quickly identify implemented controls for assessment along with the applicable assessment objectives and procedures to be utilized in a single view.
- TA provides mobility support allowing the analysts to interview staff and conduct assessment review away from TrustedAgent, and to import the results at a later time.

MANAGE Phase

Finding and Weakness Management	87% Reduction

Most organizations rely on one or more key individuals to manage activities related to this phase and the next two phases. This person typically manages data calls to business owners, usually via phones and emails, and collects information including findings, weaknesses, and regulatory deliverables and artifacts from the various business owners. This person also aggregates the results into home-grown tools including Access applications, spreadsheets, and Sharepoint, and generates management reporting and dashboard metrics for senior management. When the number of inventory is large across the organization, i.e. exceeding 200 systems, this role tends to be delegated to multiple individuals. Based on our study, at least a full FTE can be removed from the organization by adopting automated solution. As the tool becomes mainstream and the users gain expertise with the tool, incrementally but partial FTE can also be achieved. Unfortunately this metric was not obtainable from our results.

- TrustedAgent supports finding management from failed control assessments and audits. Findings may include impacted assets, business impact analysis, risk values and mitigation.
- Where findings are imported from vulnerability assessment results, TA manages the findings and their association to the impacted assets (devices) within an inventory.
- Findings can be accepted, rejected, or linked to create corrective actions.
- TA simplifies the corrective action management process by allowing corrective actions to be created from linked findings along with all key elements.
- With finding and weakness notifications, users can stay ahead of weaknesses coming due, or when changed and ensure that findings and weaknesses are addressed in timely manner.
- TA supports the imports of findings and weaknesses using data templates for accelerating data migration from legacy processes.

AUTHORIZE Phase

Performance Metrics and Management Dashboard	95% Reduction

- TrustedAgent supports performance metrics such as statuses and key due dates for key security deliverables such as ATO, SSP, SAR, etc. Artifacts can be tracked enabling real-time review and verification. TA also provides notification support and visual indications to ensure timely management of the metrics.
- TA dashboard organizes key metrics into views relating to Authorization, Inventory, Assets, Controls, Findings, and Corrective Actions. These views are provided with filters and drillable details allowing visualization of information in an easy to understand manner.

Regulatory Document Generation	90% Reduction

- TrustedAgent automates the generation of many core documents for security authorization based on organization-defined format on a real-time basis. The automation saves significant time for many organizations. For example, FISMA would require a minimum of five core documents, while FedRAMP requires 16 core documents. Without an automation framework, the same process would require endless iterations of editing and update any time information is changed. This effort addresses organization-specific information, common controls, control implementation and testing, identified findings, risk level, business impact analysis, corrective actions, and appendices.
- TA supports a variety of reports including Cyberscope and OMB's Plan of Action and Milestones reports as well as the capability to execute ad hoc reports to support data calls.

MONITOR Phase

Continuous Monitoring	91% Reduction

- TrustedAgent supports continuous monitoring by enabling the ability for selected controls to be retested for effectiveness during the assigned monitoring period. TA also supports the retesting of controls due to system modification, verification of weakness remediation for closure, or any other key reasons.

- TA offers vulnerability assessment scheduling to conduct scans on demand or as scheduled for supported vulnerability scanning applications (SAINT or OpenVAS).
- TA manages assets updated from vulnerability management scans as required for change.

Financial Model for Justification of TrustedAgent GRC

In this part of our white paper, we propose a quantitative technique to provide measureable and cost justifications to senior management to support the acquisition of TrustedAgent to replace manual methods supporting security authorization.

Consider the following scenario in the justification. An organization with requires an enterprise deployment of TrustedAgent to manage security authorization across for 30 systems of Moderate level. The organization intends to host TrustedAgent in its data center using acquired hardware and software with rooms to support future growth.

FINANCIAL MODEL FOR JUSTIFICATION OF TRUSTEDAGENT GRC

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

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

Using the metrics discussed from the study, it is then possible to derive cost savings vs. manual methods for the activities using TrustedAgent. The savings are annualized similar to the initial investment and recurring expenses by the organization.

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

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

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

The results demonstrated in the above model are consistent in IRRs and breakeven noted in other studies including the one quoted in this paper.

Conclusion

The highly scalable and customizable TrustedAgent provides the optimal solution for any organization seeking a balance of between cost, expected requirements, and implementation time. Using the outlined measures, organizations can present plausible and quantifiable business cases to support the acquisition of GRC solutions.

Just as equally as important as having tangible justifications, organizations must not forget, that due to the complexity of GRC processes and their applicability, not all justifications can be measured in dollars and cents. Organizations should also take into considerations the intangibles including:

- Integration of key GRC process under one centralized risk management framework, allowing the organization to manage compliance and risk activities under one comprehensive, standardized, and enterprise-wide approach.

- Elimination of information silos and duplications of compliance activities.
- Gain visibility and timely access to information to support clear, data-oriented risk-based decisions.

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